Internetworking With CISCO Routers

Course Outline

MSTP

- Intro to Routing
- Router Interfaces
- Cisco Discovery Protocol (CDP)
- Routing
  - Static Routes
  - Distance Vector Routing
  - Link State Routing
  - Dynamic Routing
- Security Issues
- Advanced Topics

Graphic Symbols

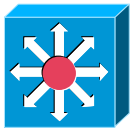

Bridge


Switch

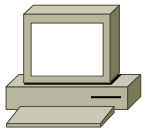

Router


Access server


ISDN switch

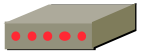

Multi-layer switch


Network switch


Personal computer

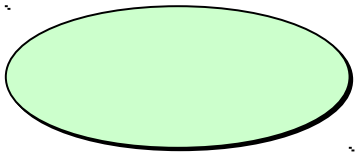

File Server

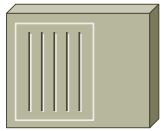
Data Service Unit/ Channel Service Unit

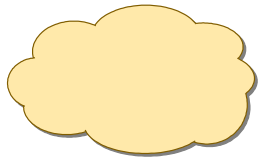

Modem

Web Server


WAN “cloud”


VLAN (Color May Vary)


Hub


Network Cloud or Broadcast Domain

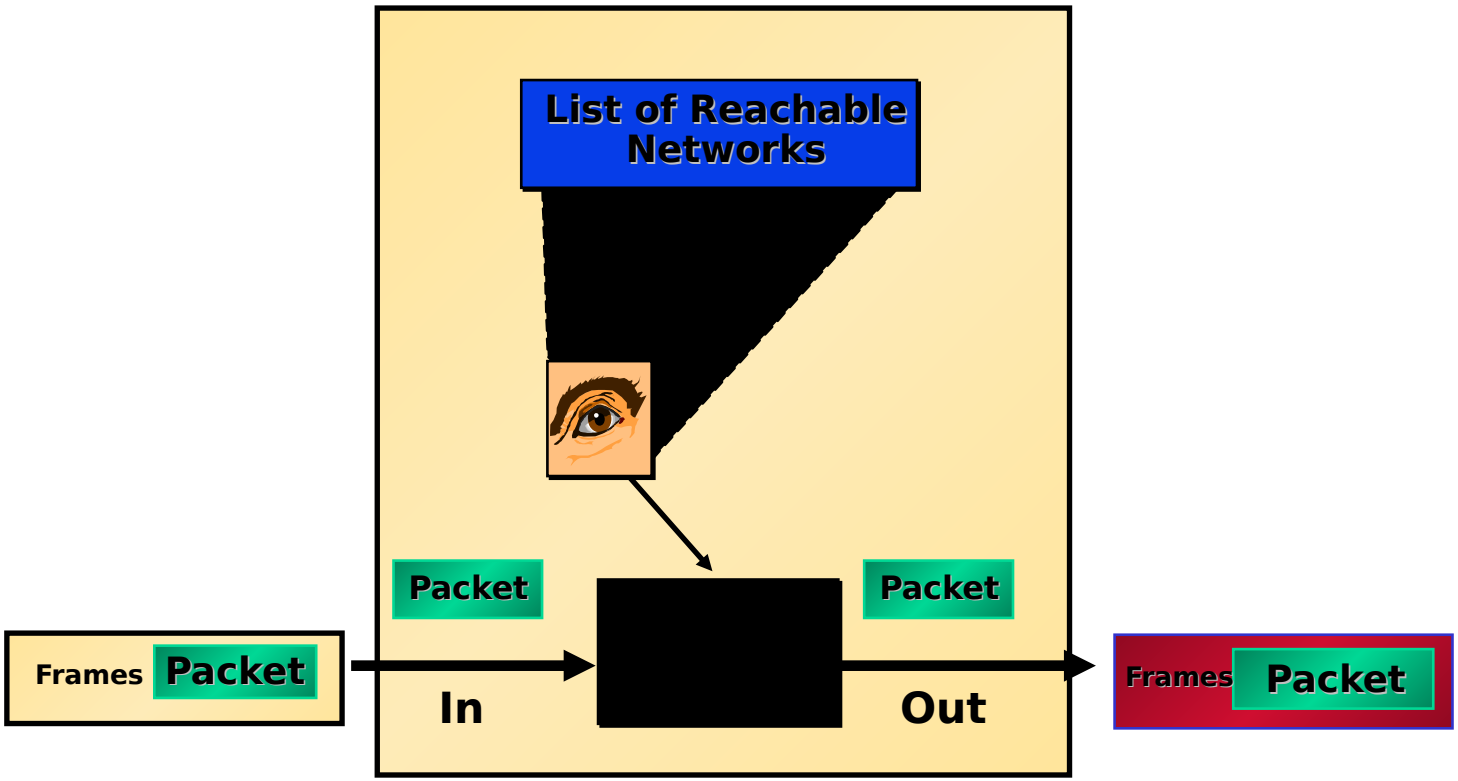
Ethernet


Fast Ethernet

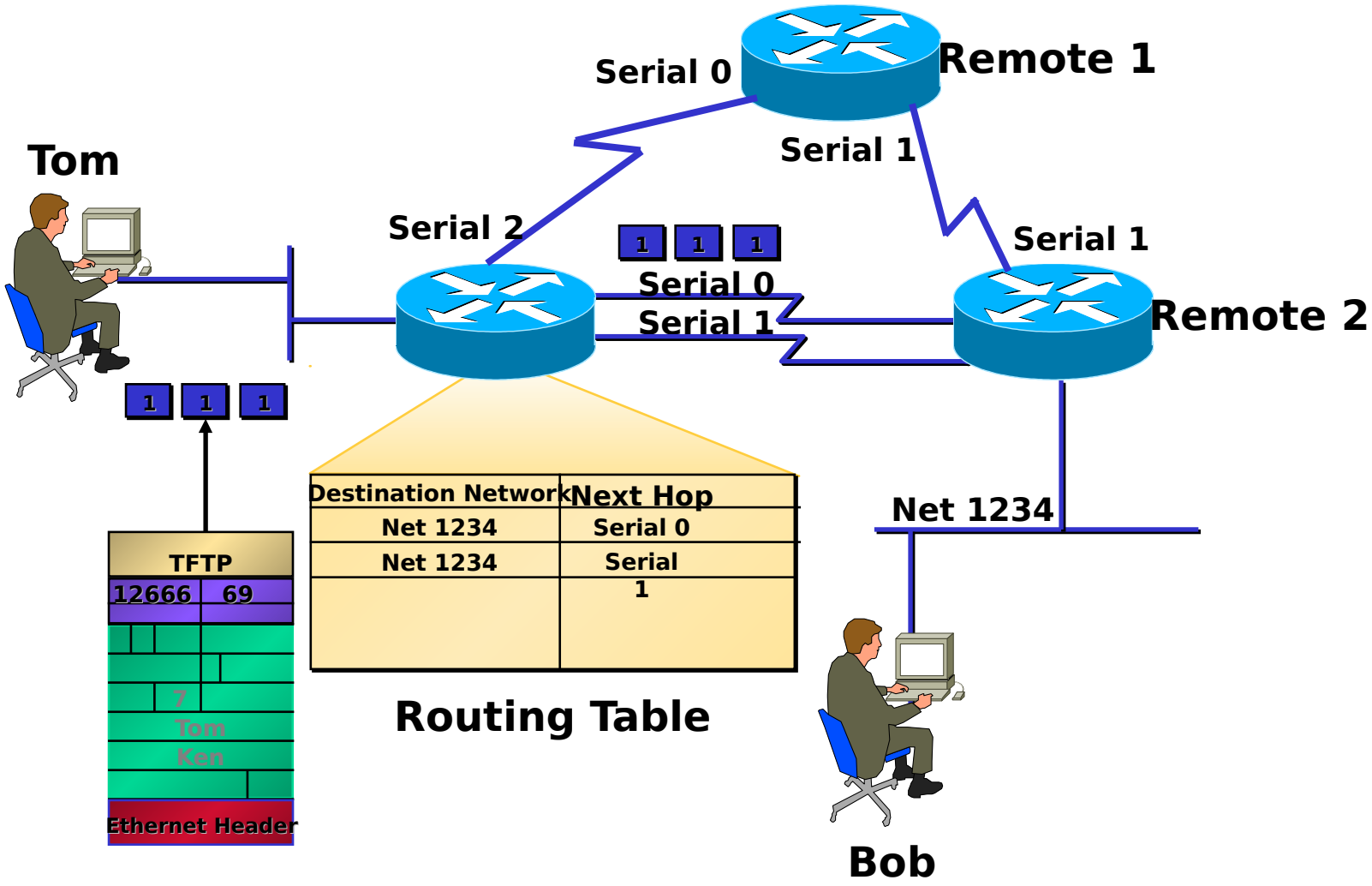

Serial Line


Circuit Switched Line

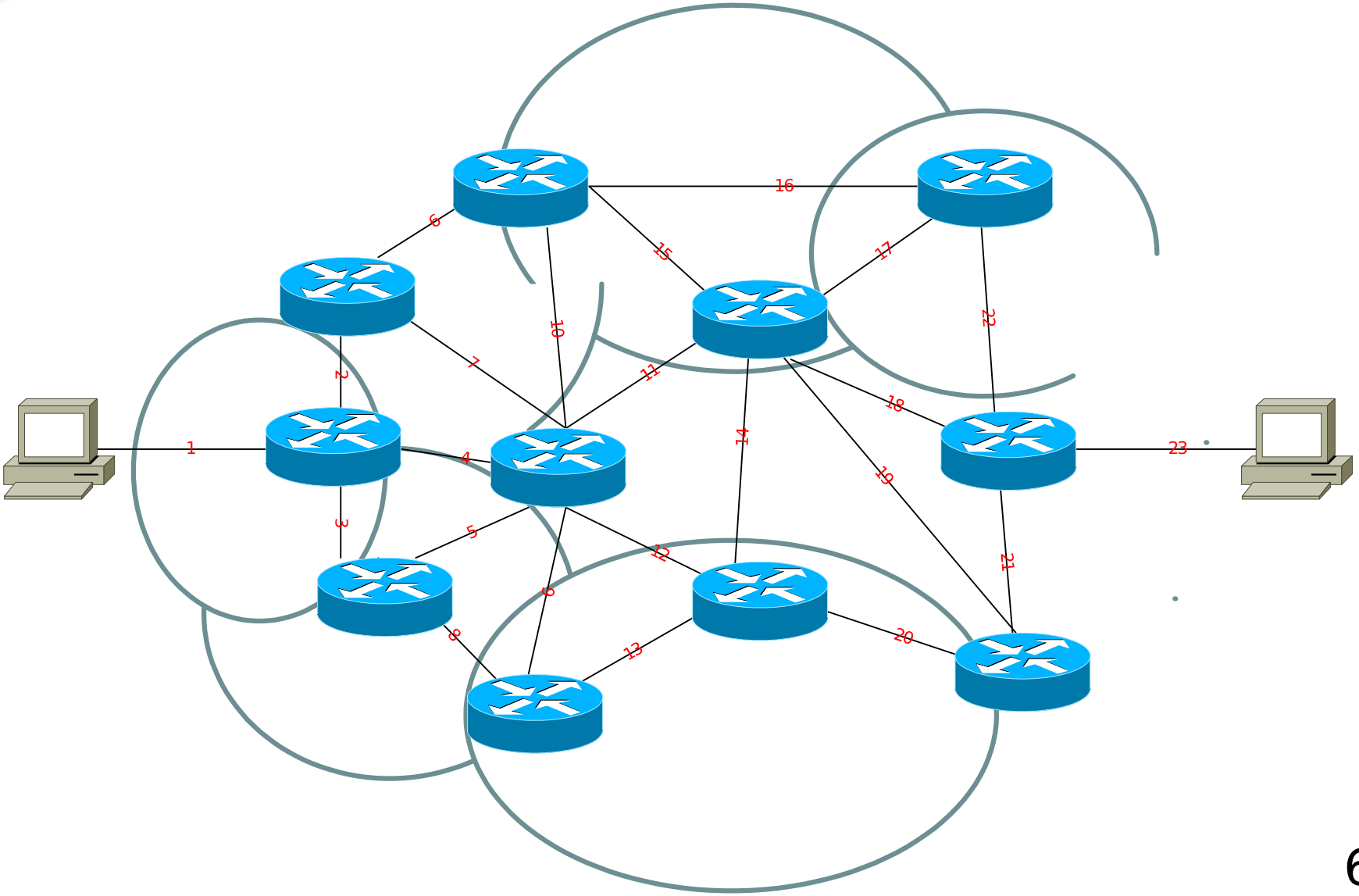
What is a Router?



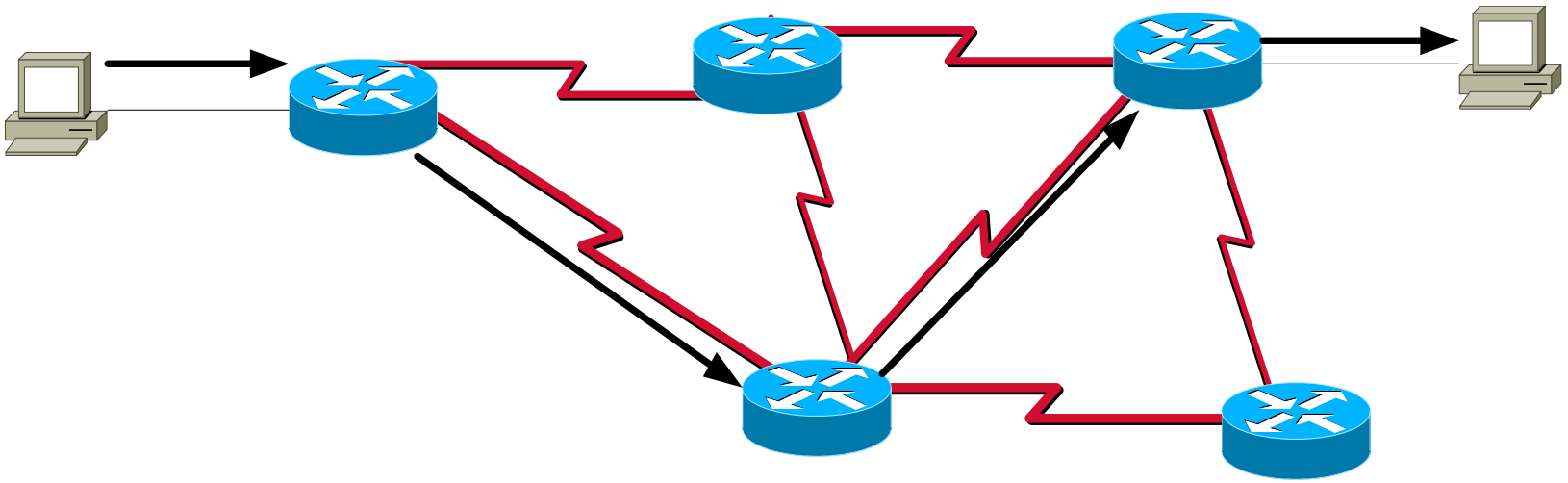
Which Path?

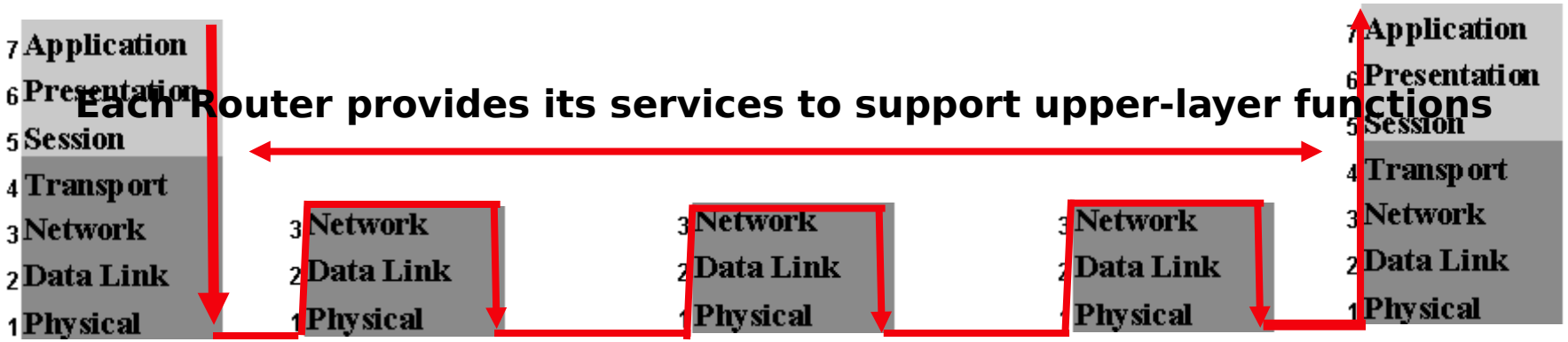

Serial 0
Remote 1
Serial 1
Tom
Serial 2
1 1 1
Serial 0
Serial 1
Serial 1
Remote 2
1 1 1
Destination Network
Next Hop
Net 1234
Serial 0
Net 1234
Serial 1
Net 1234
TFTP
12666
69
7
Tom
Ken
Ethernet Header
Routing Table
Bob

Communicate Path

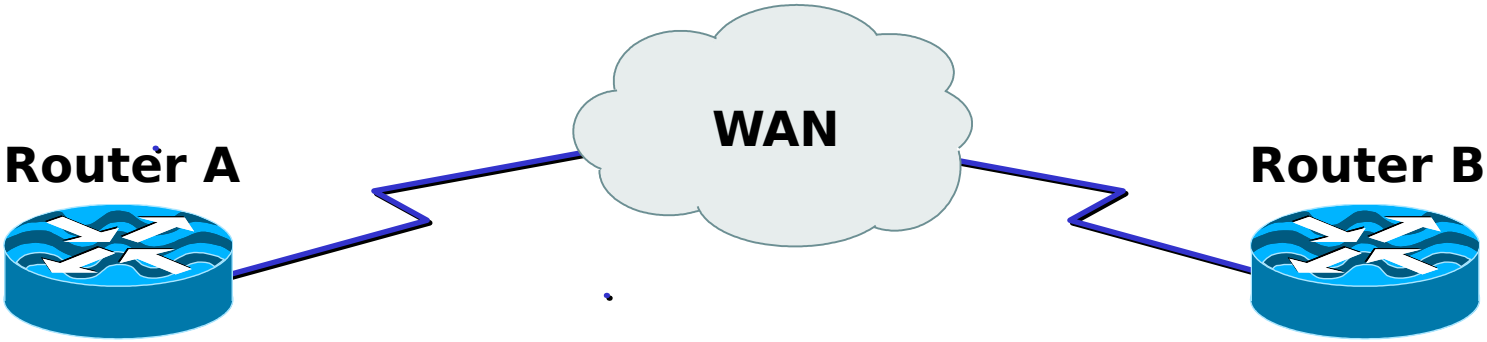


Network Layer Protocol Operations



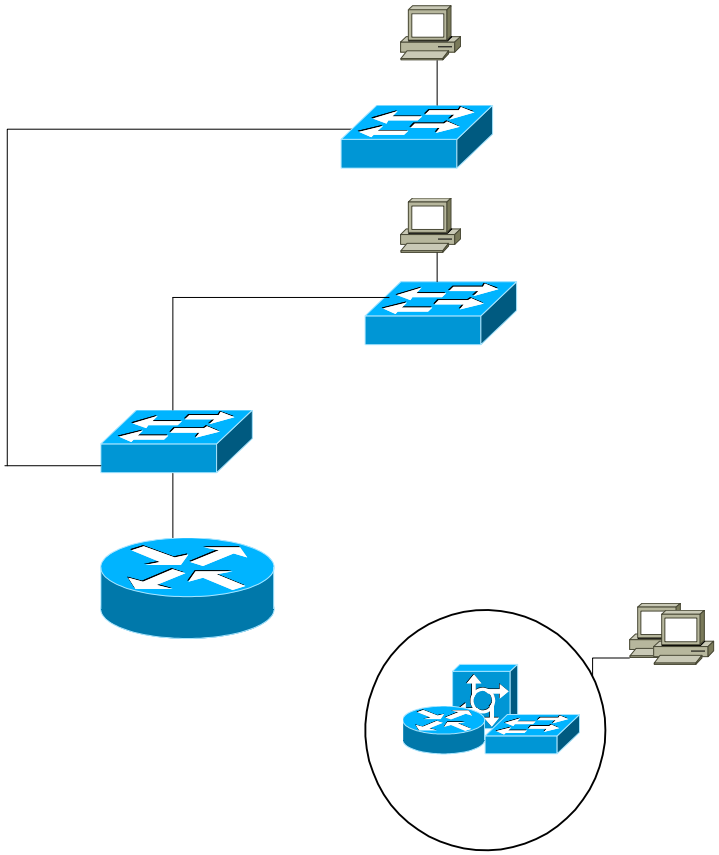


What do Routers do?



- Routers gather and maintain routing information to enable the transmission and reception of IP Datagrams
- Routing information is kept in a routing table
  - One entry for each known route
- Routers can create and maintain the routing table dynamically to accommodate network changes as they occur
- The rules for the exchange of routing information amongst routers are called routing protocols

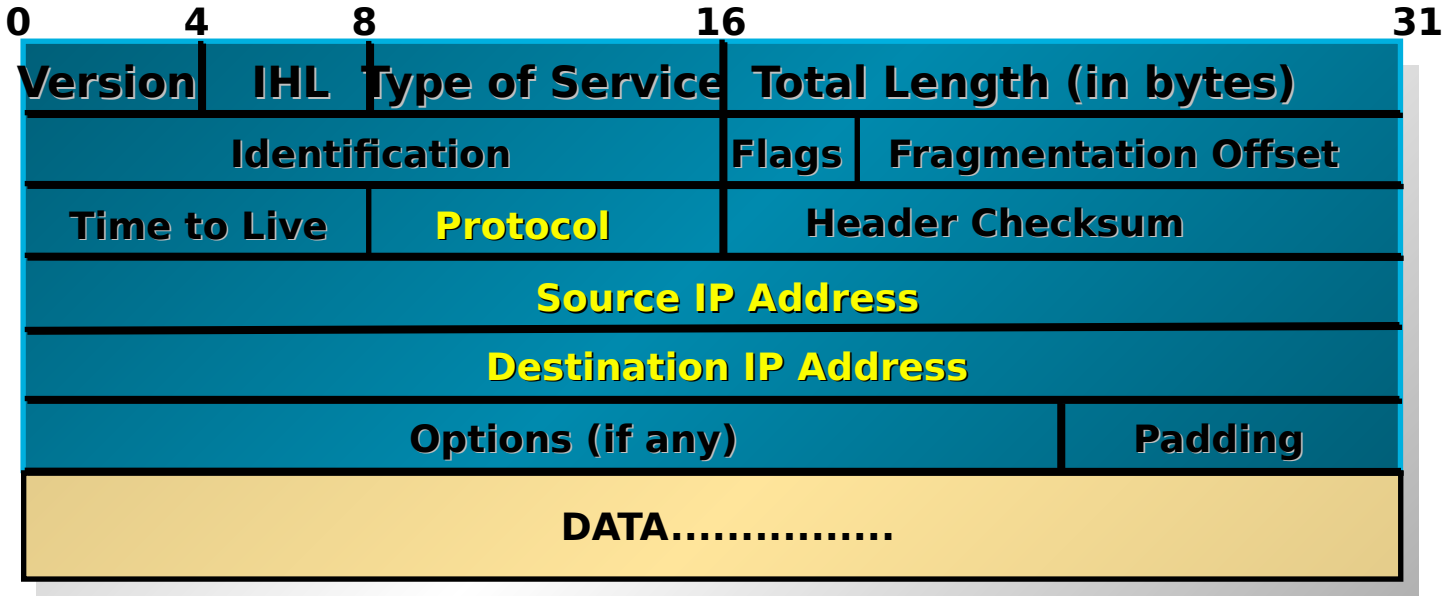
What do Routers do?



- Broadcast Control
- Multicast protocol
- Optimal Path determination
- Traffic Management
- Connects to WAN services

- **How do they do this?**

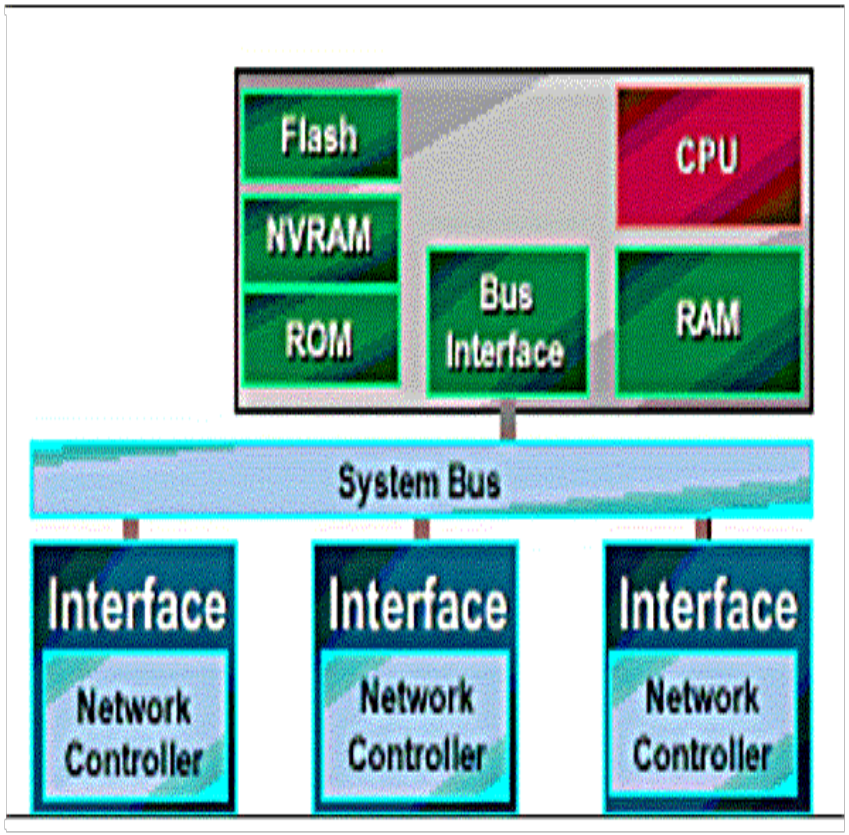
IP Header and Protocol Numbers



Number	Protocol
1	ICMP—Internet Control Message Protocol
2	IGMP—Internet Group Message Protocol
6	TCP—Transmission Control protocol
7	UDP—User Datagram Protocol

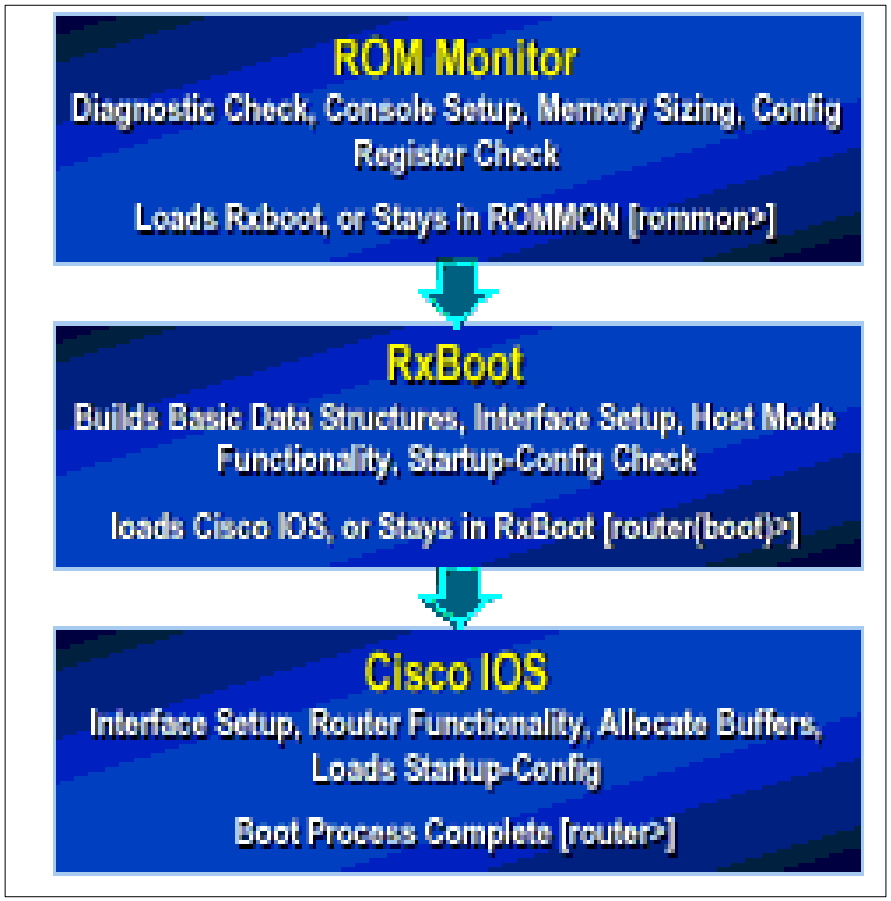
Let’s break down the router

ROM, Flash, NVRAM and RAM



- ROM: Stores the bootstrap program and POST
- NVRAM: Non-volatile RAM holds the router configuration
- FLASH: (EEPROM) holds the Cisco IOS (Inter networking Operating System)
- RAM: Provides caching and packet buffering

Router boot up



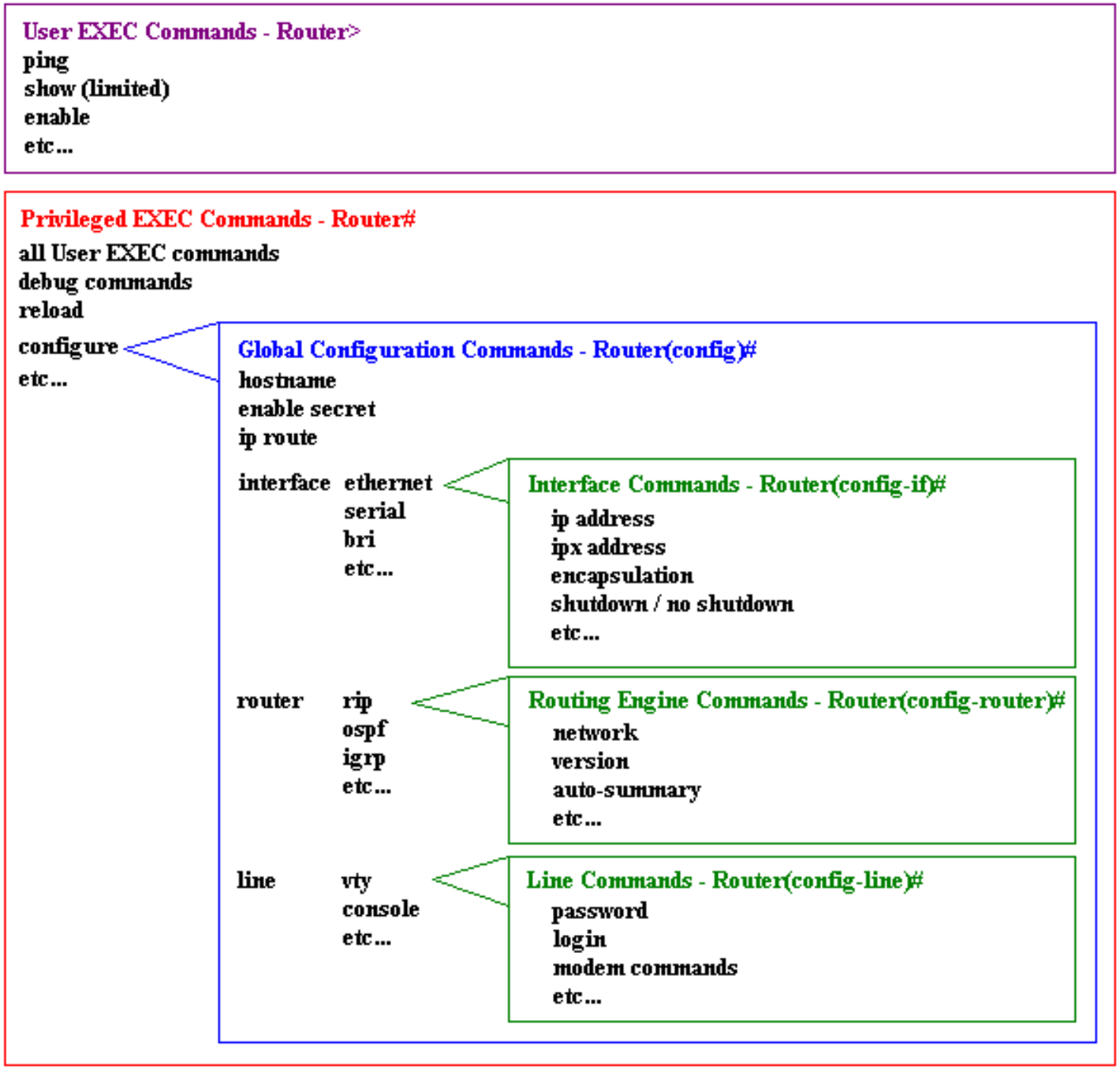
- ROM Monitor:
  - Loads bootstrap, Reboots, or Stays in RMOM
- RxBoot:
  - Locates and loads the system IOS
- Cisco IOS:
  - Locates and loads the configuration file or enters auto setup

First-time System Startup > Ver 11.3

- Before you start, be aware of the following:
  - Which protocols you plan to route
  - Types of interfaces installed (Ethernet,Serial...)
  - Whether or not you plan to use bridging
- Step 1: Attach an RS-232 ASCII terminal, or straight-thru cable, to the system console port located at the rear of the router.
- Step 2: Configure the terminal to operate at 9600 baud, 8 data bits, no parity, 1 stop bit.
- Step 3: Power on the router and watch startup

Entering System Prompt

- There are three ways to get into the system on the router.
  - Use the router console port
  - Telnet into a virtual port
  - Use modem on aux port


User EXEC Commands - Router>
ping
show (limited)
enable
etc...
Privileged EXEC Commands - Router#
all User EXEC commands
debug commands
reload
configure
etc...
Global Configuration Commands - Router(config)#
hostname
enable secret
ip route
interface
ethernet
serial
bri
etc...
Interface Commands - Router(config-if)#
ip address
ipx address
encapsulation
shutdown / no shutdown
etc...
router
rip
ospf
igrp
etc...
Routing Engine Commands - Router(config-router)#
network
version
auto-summary
etc...
line
vty
console
etc...
Line Commands - Router(config-line)#
password
login
modem commands
etc...

Configuration Process

- Lock down the Router
  - Line Con 0, Line VTY 0 4, Line Aux 0, and Enable Secret
- Configure the Identity
  - Host name, Services, and Banners
- Configure the Interfaces (Inside/Outside)
  - Ethernet / Serial Interfaces
- Configure Routing Protocols (Inside/Outside)
  - Internal Routing Protocols (RIP, IGRP, EIGRP)
  - External Routing Protocols (BGP, EIGRP)
- Configure Advanced parameters
  - QoS

Lock Down the Router

Router(config)#line con 0

Router (config-line)#login

Router (config-line)#password *your-password*

Router(config)#line aux 0

Router (config-line)#login

Router (config-line)#password *your-password*

Router (config)#line vty 0 4

Router (config-line)#login

Router (config-line)#password *your-password*

Router (config)#enable secret *your-password*

Configure the Identity

Router (config)#hostname *IMEF*

IMEF (config)#service timestamps debug date

IMEF (config)#service timestamps log date

IMEF (config)#service password-encryption

IMEF (config)#clock timezone EST 5

IMEF#clock set 16:27:00 May 22 2002

IMEF (config)#banner motd #

IMEF (config)#banner login #

Configure Interfaces (Inside/Out)

IMEF(config)#interface fa 0/1

IMEF(config-if)#description LAN to I MEF Servers

IMEF(config-if)#ip address 192.168.25.33 255.255.255.224

IMEF(config-if)#media-type 10BaseT (if required, 4500)

IMEF(config-if)#no shut

Configure Interfaces (Inside/Out)

IMEF(config)#interface Serial 0/1

IMEF(config-if)#description WAN Connection to 1st Marine Division

IMEF(config-if)#ip address 192.168.21.5 255.255.255.252

IMEF(config-if)#encapsulation ppp

IMEF(config-if)#clock rate 512 (only DCE interfaces)

IMEF(config-if)#no shut

Configure Routing Protocols (Inside/Out)

- Configuring Internal Routing Protocols
  - IMEF(config)#Router RIP
  - IMEF(config-router)#network 192.168.25.0
  - IMEF(config-router)#network 192.168.21.0
  - IMEF(config)#Router BGP 2550
  - IMEF(config-router)#neighbor 192.168.21.6 remote-as 3550
  - IMEF(config-router)network 192.168.25.0 mask 255.255.255.0

Configure Advanced Parameters

- Quality of Service (QoS)
  - First In First Out (FIFO)
  - Priority Queuing
  - Custom Queuing
  - IP Precedence
  - Weighted Fair Queuing
  - Class Based Weighted Fair Queuing
  - Fragmentation with Interleave

Editing in the Configuration Mode

- Delete or Backspace - Erases one character
- Ctrl-W - Erases a word
- Ctrl-U - Erases a line
- Ctrl-R - Redisplays a line
- Return - Executes single-line commands
- Ctrl-Z - Ends configuration mode and returns to the EXEC prompt

See Router Configuration

- Show startup-config shows the configuration in NVRAM
  - sh start
- Show running-config shows the configuration that is currently running
  - sh run

Saving and Restoring the Config

- Copy/Back up your configurations!!!!!!!
  - Copy run start (write mem)
  - Write network
  - Copy start (run) tftp
  - Copy run (filename)
- Load backup from network
  - Config network {*memory, terminal}*
- TFTP, Network Management, Logging – ***A MUST!***

TFTP Server

The Cisco TFTP server application provides Trivial File Transfer Protocol (TFTP) server functionality on Windows 95, Windows 98, Windows NT, and Windows 2000 operating systems. Using the TFTP server application with TFTP client software, you can transfer files from one location to another.

"Show Version"

Information found from "show version"

- Operating System
- Router model and processor revision
- System Image file name
- Amount of memory
- Software set (Enterprise)
- Amount of Flash memory

Cisco Internetwork Operating System Software

IOS (tm) 4000 Software (XX-I-M), Version 10.3(2), RELEASE SOFTWARE (fc1)

Copyright (c) 1986-1995 by cisco Systems, Inc.

Compiled Wed 29-Mar-95 12:11 by chansen

Image text-base: 0x00012000, data-base: 0x002C28E0

ROM: System Bootstrap, Version 4.14(7), SOFTWARE

4000-B uptime is 23 minutes

System restarted by power-on

System image file is "xx-i-mz.103-2", booted via flash

cisco 4000 (68030) processor (revision 0xB0) with 32768K/16384K bytes of memory.

Processor ID 5030279

G.703/E1 software, Version 1.0.Bridging software.

X.25 software, Version 2.0, NET2, BFE and GOSIP compliant.

4 Ethernet/IEEE 802.3 interfaces.

4 Serial network interfaces.

128K bytes of non-volatile configuration memory.

8192K bytes of processor board System flash (Read/Write)

Cisco Banners

- MOTD – Message of the Day
  - Router#banner motd #
    Stop! Government site
    #
- Incoming
- Exec
- Login

Internetworking Cisco Routers
Lab 1
IOS Commands

30 Min.

Configuring Interfaces

- Ethernet interfaces

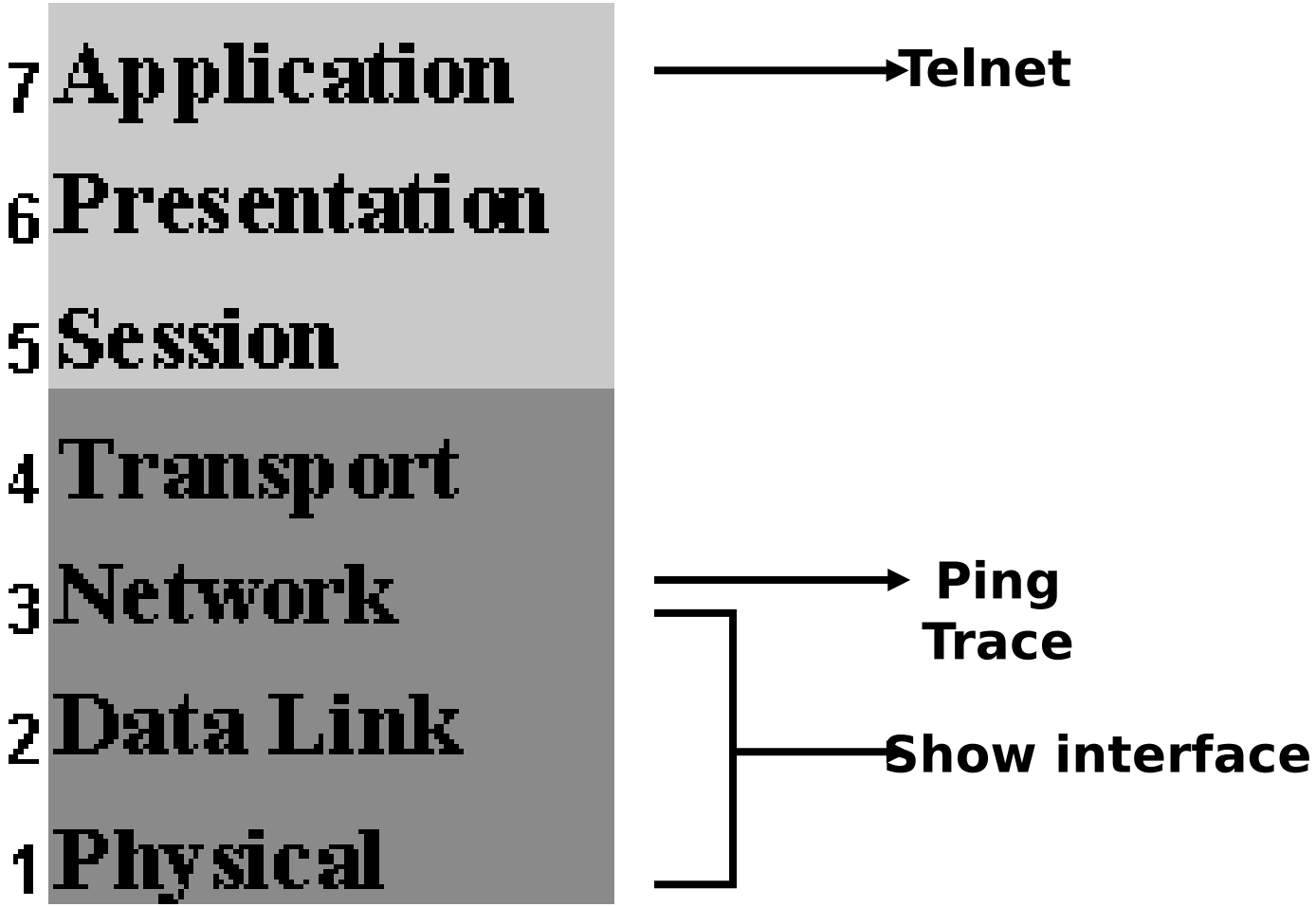
```
config t
int e0
description MITNOC LAN
ip address 192.168.21.33
255.255.255.224
media-type 10baset
no shut
end
copy run start
```

Configuring Interfaces

- Serial interfaces

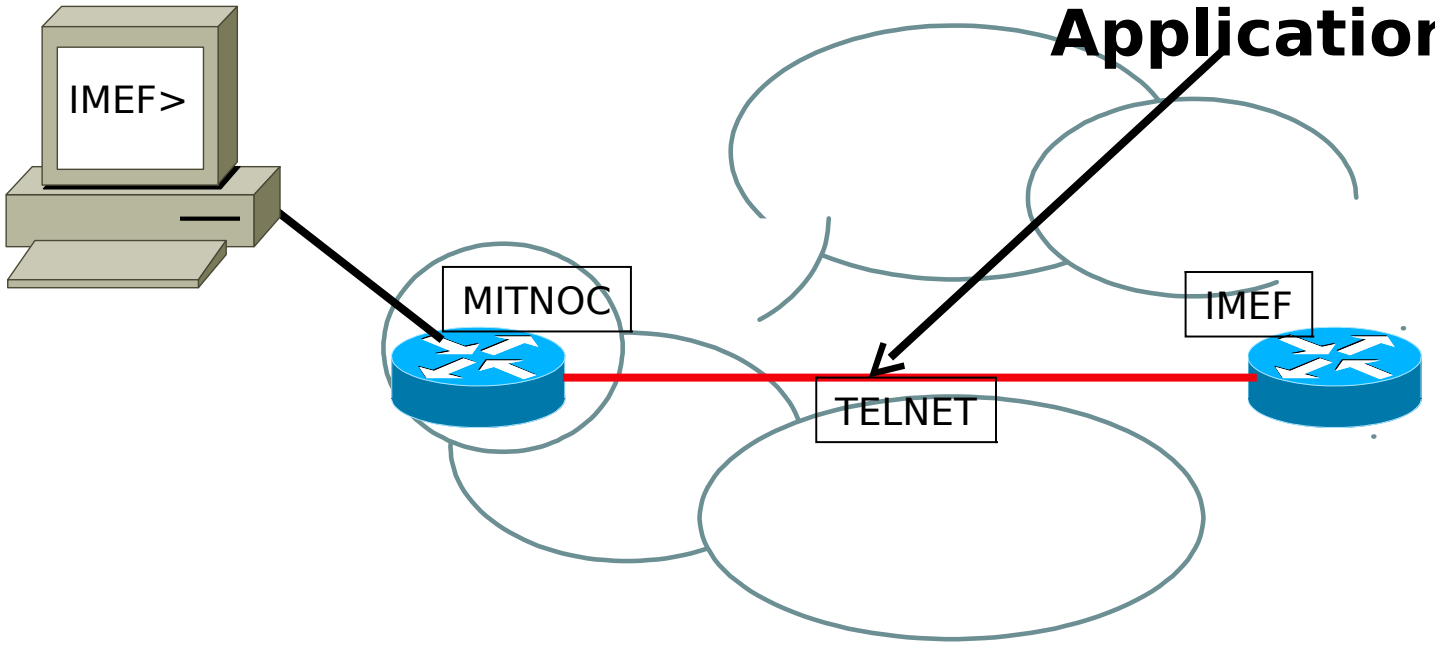
```
config t
int s0
description Wan connection to
III MEF
ip address 192.168.20.21
255.255.255.252
clock rate 56000
no shut
end
copy run start
```

Testing Overview



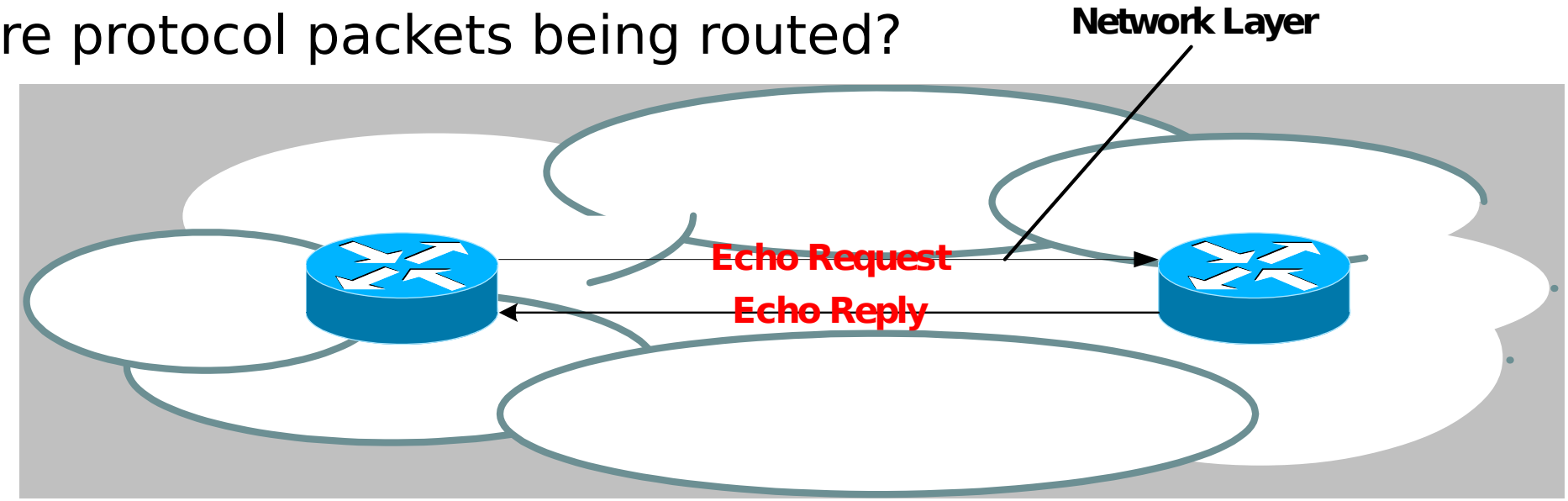
Test Application Layer using Telnet

Can the remote router be accessed?



Testing with the *Ping Command*

Are protocol packets being routed?

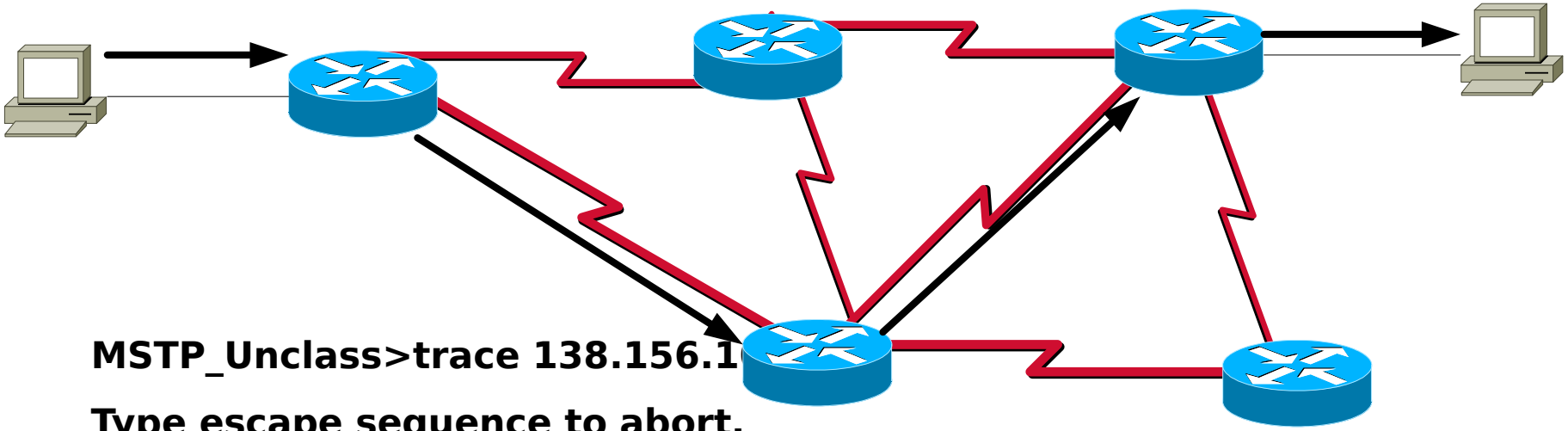



```
MSTP_Unclass>ping 138.156.100.252

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 138.156.100.252, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
MSTP_Unclass>
```

Testing with *trace* command

hat path are packets taking?



MSTP_Unclass>trace 138.156.1

Type escape sequence to abort.

Tracing the route to mqg-dns1.quantico.usmc.mil (138.156.100.252)

1 138.156.169.1 0 msec 0 msec 4 msec

2 mqg-dns1.quantico.usmc.mil (138.156.100.252) 0 msec * 0 msec

MSTP_Unclass>

Viewing Routing Information

Show IP route

Clear IP route *

```
router#sh ip rou

Codes: I - IGRP derived, R - RIP derived, H - HELLO derived, O - OSPF derived
       C - connected, S - static, E - EGP derived, B - BGP derived
       * - candidate default route, IA - OSPF inter area route
       E1 - OSPF external type 1 route, E2 - OSPF external type 2 route

Gateway of last resort is 143.211.250.9 to network 0.0.0.0

     143.211.0.0 is subnetted (mask is 255.255.255.0), 44 subnets
C       143.211.92.0 is directly connected, Ethernet12
C       143.211.93.0 is directly connected, Ethernet13
R       143.211.152.0 [120/1] via 143.211.200.250, 0:00:27, Ethernet5
C       143.211.155.0 is directly connected, Ethernet8
R       143.211.136.0 [120/1] via 143.211.135.10, 0:00:22, Ethernet4
```

Clearing Statistics and Tables

- Clear Counters - Resets all counters on the interface stats. Useful if trying to troubleshoot an interface.
- Clear IP Route * - Clears all known IP routes from the table, forcing them to relearn. Useful when setting up the network to ensure changes take place.
- Clear IP Cache - Clear IP cache table, which goes along with the "clear ip route" command.
- Clear ARP - Useful if changing IP addresses among workstations on the same line, to ensure that the router does not have a bad entry.

Interpreting *show interface serial*

MSTP

Router# show int s 1

Serial1 is up, line protocol is up

Hardware is cxBus Serial

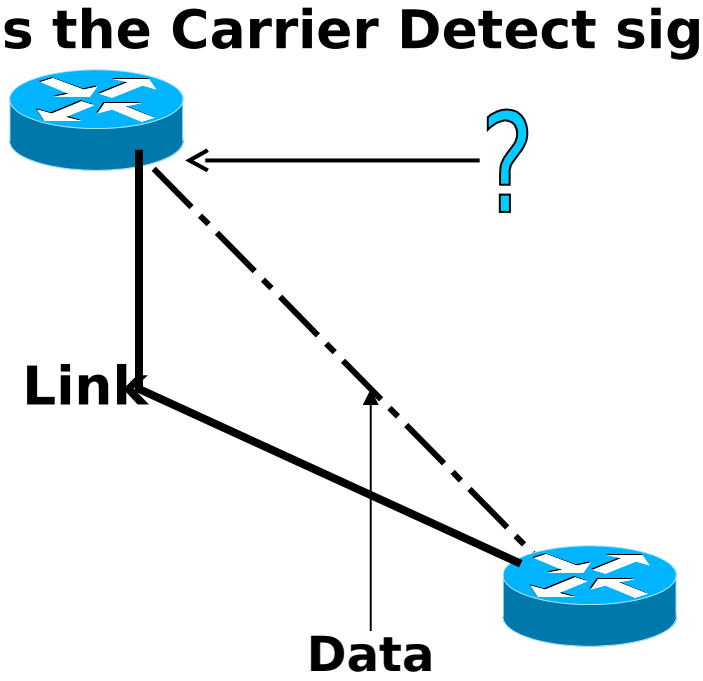
Keepalives

Carrier Detect

Operational……	**Serial1 is up, line protocol is up**
Connection Problem……	**Serial1 is up, line protocol is down**
Interface Problem……	**Serial1 is down, line protocol is down**
Disabled……	**Serial1 is administratively down, line proto**

Is the Link Operational?

- Hardware (Physical Layer)
  - Cable
  - Connectors
  - Interface
- Data Link Layer
  - Keepalive Messages
  - Control Information
  - User Information



Interpreting Serial Interface Errors

- Input errors (1): CRC, frame, overrun, abort
  - Rule of thumb: Input errors should not exceed approximate range of 0.5 to 2.0 percent of interface traffic
- CRC errors
  - Indicates packet received does not match packet sent
  - Caused by some type of interference on transmission link
  - Possible causes:
    - **Faulty cables, cable too long, unshielded cables**
    - **“Dirty” telco circuits**
    - **CSU/DSU clocking problems**

Interpreting Serial Interface Errors

- Framing Errors
  - Indicates packet received does not end on 8-bit byte boundary
  - Similar causes to CRC errors
  - Also caused when CSU/DSU coding and framing parameters do not match line parameters
  - Ensure all devices are using same clock source
- Overruns
  - Occur (rarely) when packets arrive too quickly for router to handle
- Aborted Transmissions
  - Indicates that an illegal sequence of bits has been received
  - Typically caused by an interface reset during a transmission
  - Many possible causes of interface resets

Interpreting Serial Interface Errors

- Interface resets
  - Indicates that a keepalive was not received when expected
    - Possible causes:
      - Constant carrier transitions
      - CSU/DSU hardware problems
      - Significant input errors
- Carrier Transitions
    - Indicates that carrier detect (DCD) signal has changed state
    - Possible causes:
      - Circuit faults (check CSU/DSU for alarms)
      - CSU/DSU hardware problems

Interpreting Serial Interface Errors

- Output queue drops
  - Indicated if no buffers are available when system is attempting to hand data off to a transmit buffer
  - Some layer 3 protocols are more tolerant of output drops than others
  - If layer 3 protocol retransmits, this increases network load
  - Always prefer output drops to be zero (or very infrequent)
- If output drops are increasing regularly
  - General indication that router cannot handle output stream
  - May be caused by saturated link
    - Only remedy for this is to buy more bandwidth

Important Info from Interface Stats


```
HoStage# show  interface  ethernet 5

Ethernet 5 is up, line protocol is up
  Hardware is cBus Ethernet, address is 0000.0c06.4ae5 (bia 0000.0c06.4ae5)
  Description: Harbrinder Network Connection
  Internet address is 192.150.42.126, subnet mask is 255.255.255.248
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec, rely 255/255, load 1/255
  Encapsulation ARPA, loopback not set, keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 4:00:00
  Last input 0:00:08, output 0:00:04, output hang never
  Last clearing of "show interface" counters 0:00:00
  Output queue 0/40, 0 drops; input queue 0/75, 5 drops
  Five minute input rate 0 bits/sec, 0 packets/sec
  Five minute output rate 2000 bits/sec, 0 packets/sec
     4703028 packets input, 605811959 bytes, 0 no buffer
     Received 184433 broadcasts, 5 runts, 0 giants
     35 input errors, 15 CRC, 15 frame, 0 overrun, 470 ignored, 0 abort
     16903029 packets output, 2249122236 bytes, 0 underruns
     0 output errors, 6577 collisions, 2 interface resets, 0 restarts
```

LAN Interfaces:Broadcast and Multicast Traffic

- Controlling broadcast/multicast traffic
  - Rule of thumb:<20% broadcasts/multicasts per segment
  - Can be calculated with (# broadcasts)/(# packets input)
  - Limit maximum number of stations per segment
  - Guidelines

Ethernet: Performance Issues

- Measuring network utilization
  - Protocol analyzers
  - User complaints
  - Rule of thumb: shared Ethernet segments <40% utilization
- Improving network utilization
  - Segmenting with routers
  - Segmenting with switches

Ethernet: Common Configuration Errors

- Cisco 4000 series Ethernet Modules
  - Supports both AUI and 10BASE-T connectors
  - AUI is enabled by default
  - 10BASE-T must be explicitly enabled

```
Router(config)#int e 0
Router(config-if)#media-type 10BaseT
```

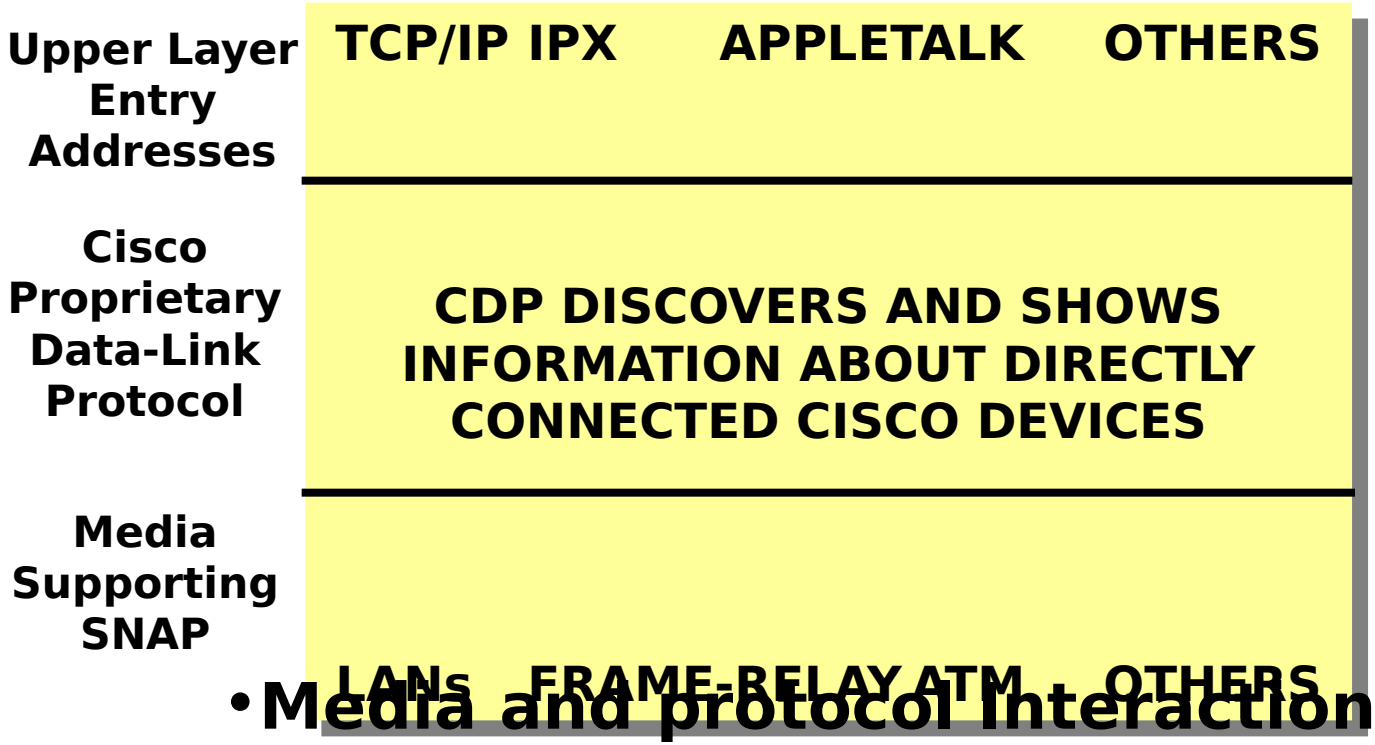
- Switch connections
  - Speed mismatch on 10/100 ports
  - Mismatch on full/half-duplex configuration
  - Incorrect cabling
    - **Crossover: switch-switch, switch-repeater**
    - **Straight: switch-router, switch-host**

Internetworking Cisco Routers

Lab 2

Interface Configuration and Testing

Cisco Discovery Protocol (CDP)



- **Media and protocol Interactions**

Cisco Discovery Protocol (CDP)

- Cisco-proprietary layer 2 multicasting protocol
- Available on all Cisco devices (with proper software release
- Media-independent
  - Runs on all media that support Subnetwork Access Protocol (SNAP) sublayer
  - LANs, Frame Relay, ATM, and others
- Protocol-independent
  - CDP packets exchanged with direct neighbors
  - Neighboring routers supporting different network protocols can
  - discover each other
- Cisco enterprise SNMP MIB available for retrieving CDP
  - information
- Enabled by default on all routers, all interfaces
  - Requires IOS 10.3+

Show CDP Neighbor Entries

MSTP_Unclass#sh cdp neigh det

Device ID: 069046783(Catalyst 5500-B-Unclass)

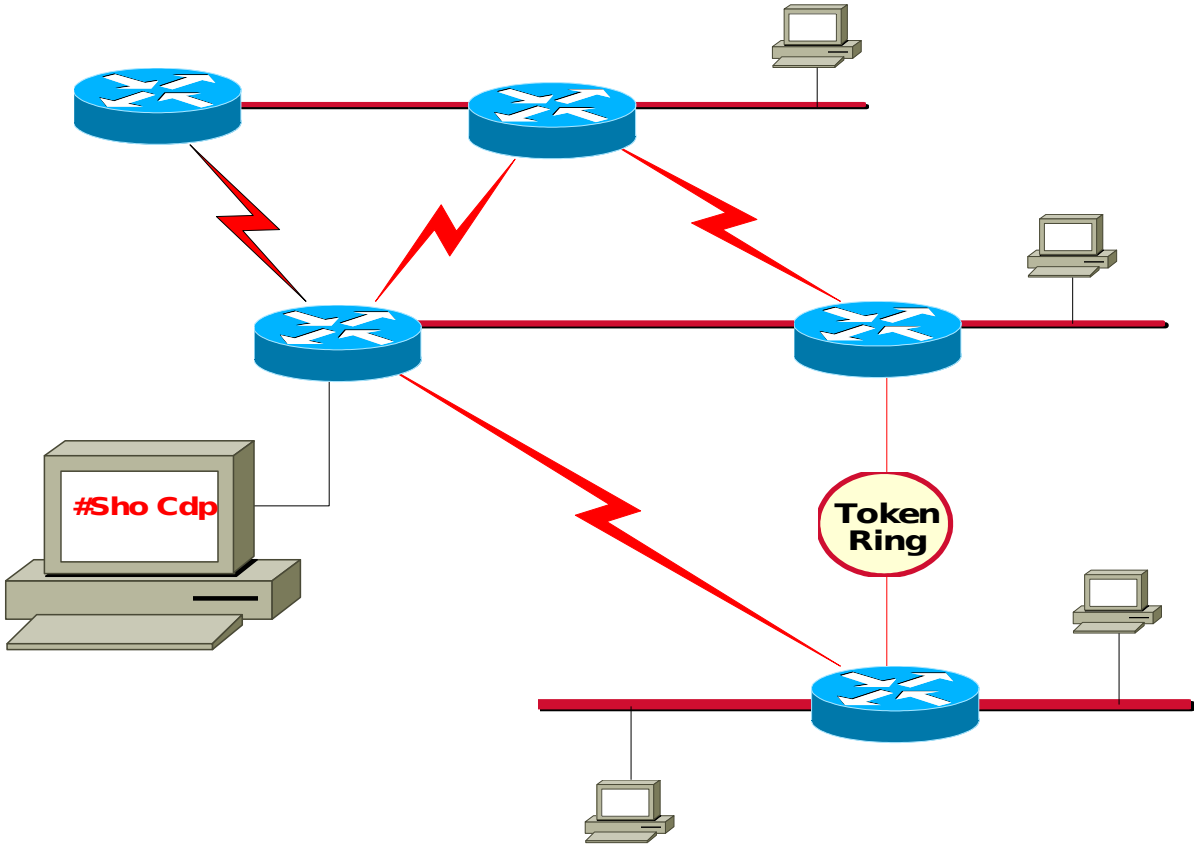
Entry address(es):

IP address: 138.156.29.2

Platform: WS-C5500, Capabilities: Trans-Bridge Source-Route-Bridge Switch

Interface: Vlan1, Port ID (outgoing port): 11/1

.....



Single command summarizes protocols and addresses on target (for example, neighboring Cisco router)

Internetworking Cisco Routers
Lab 3
Cisco Discovery Protocol (CDP)

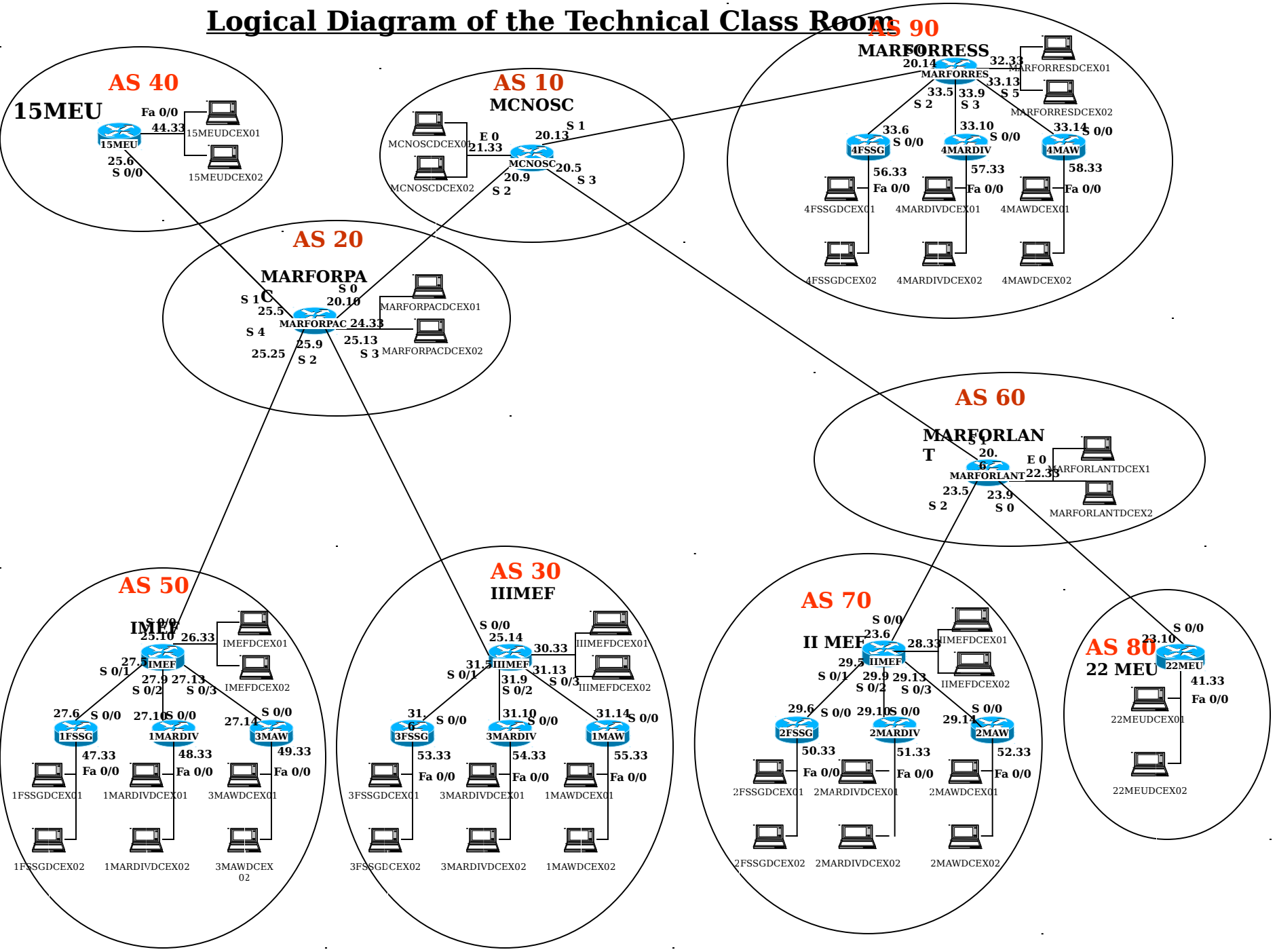
Routing

- Connected, Static, Default
- Distance Vector, Link-State
- Dynamic

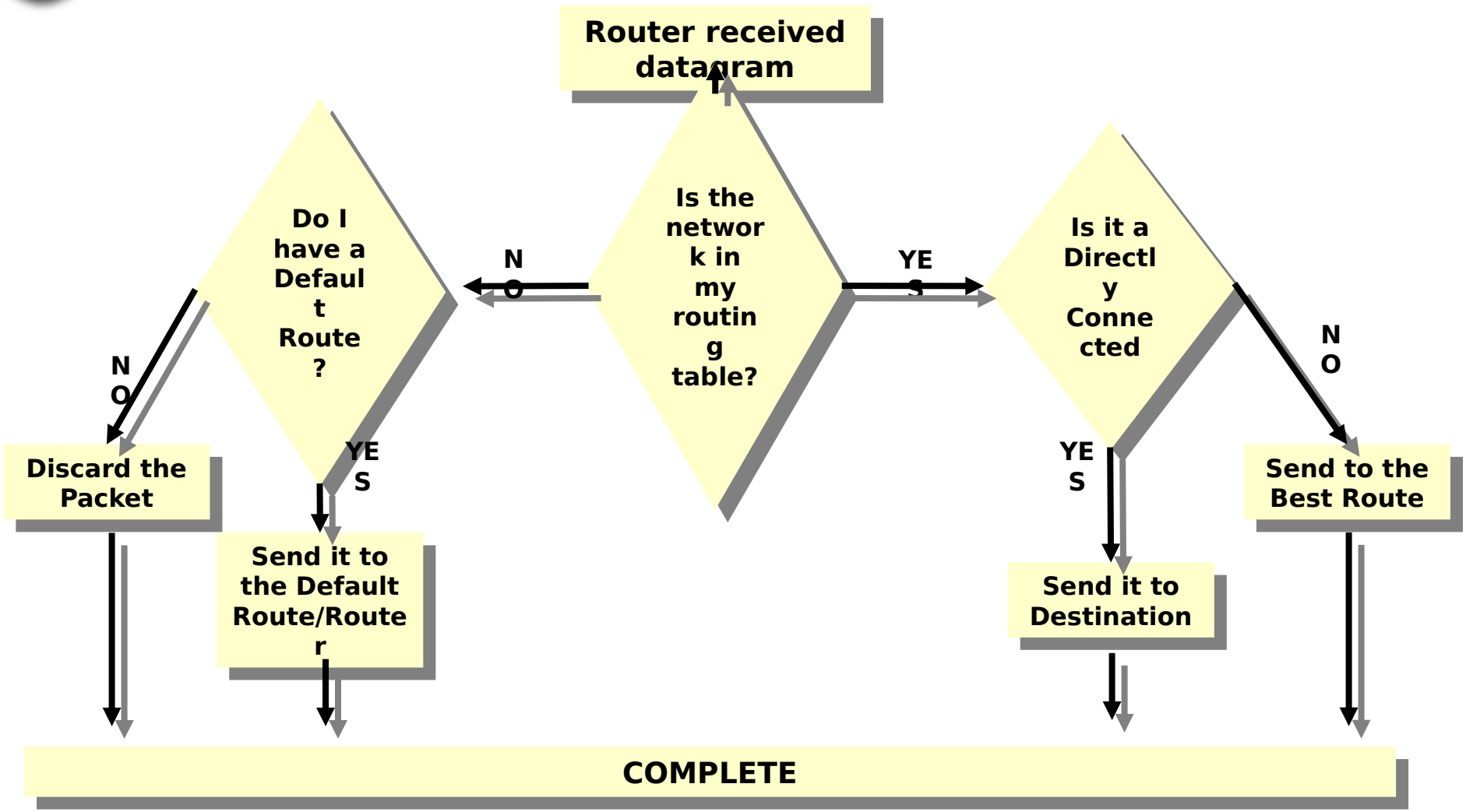
IP Routing

- Routers learn routes by:
  - Directly connected networks
  - Routing information exchange with other routers
  - Static routes
- Default router
  - Every host should have a default router defined
  - ***Default router must be reachable

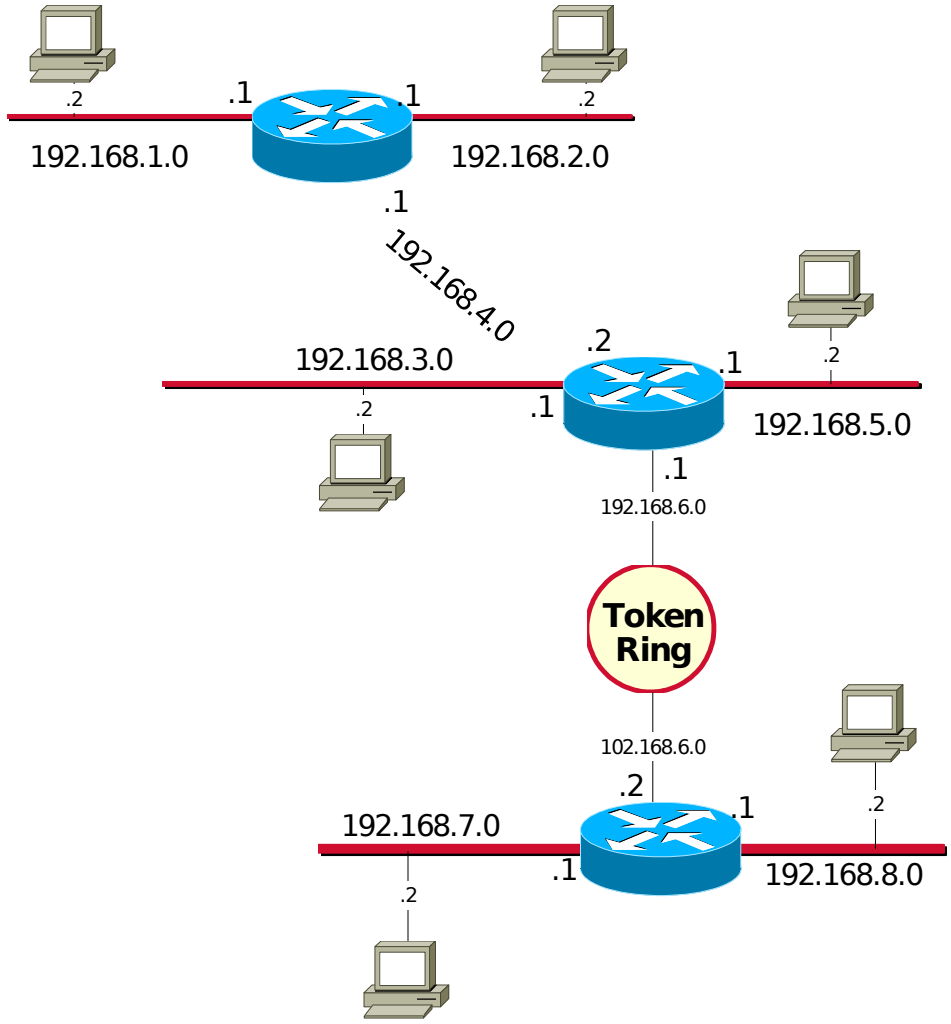
Logical Diagram of the Technical Class Room



IP Routing Process



Directly Connected Networks



ROUTE TABLE FOR ROUTER

NETWORK	VIA	HOW

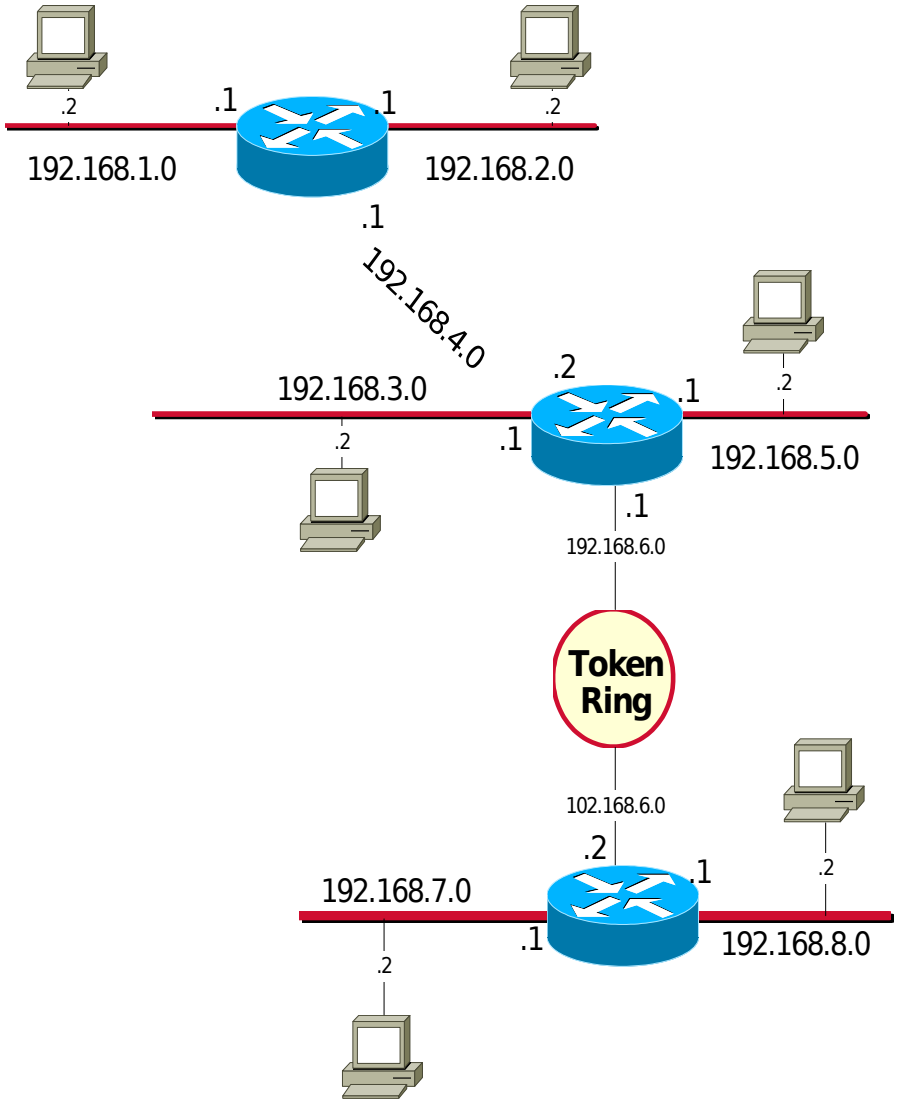
ROUTE TABLE FOR ROUTER

NETWORK	VIA	HOW

ROUTE TABLE FOR ROUTER

NETWORK	VIA	HOW

Static Routes



ROUTE TABLE FOR ROUTER

NETWORK	VIA	HOW

ROUTE TABLE FOR ROUTER

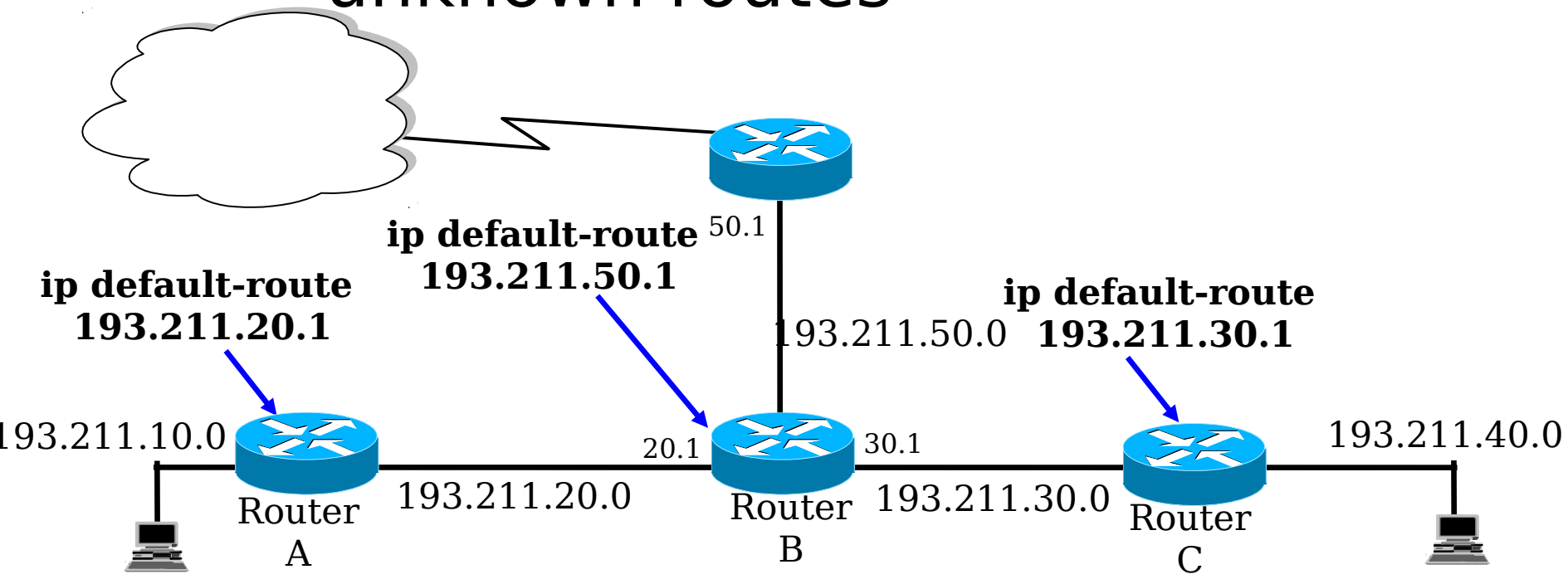
NETWORK	VIA	HOW

ROUTE TABLE FOR ROUTER

NETWORK	VIA	HOW

Default Route

Manual routes defined for unknown routes

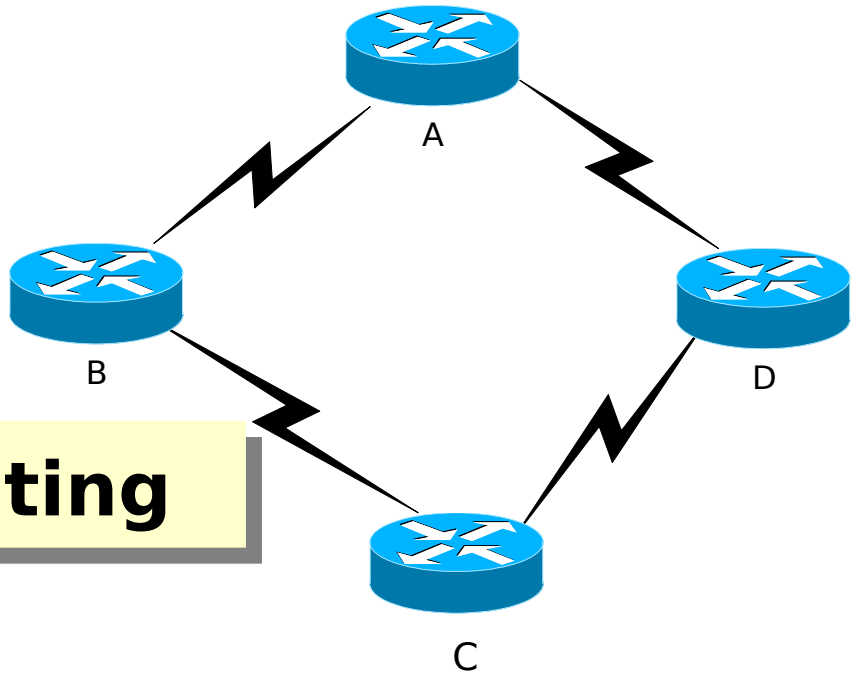


Internetworking Cisco Routers
Lab 4 Static Routes
And Lab 5 Default Routes

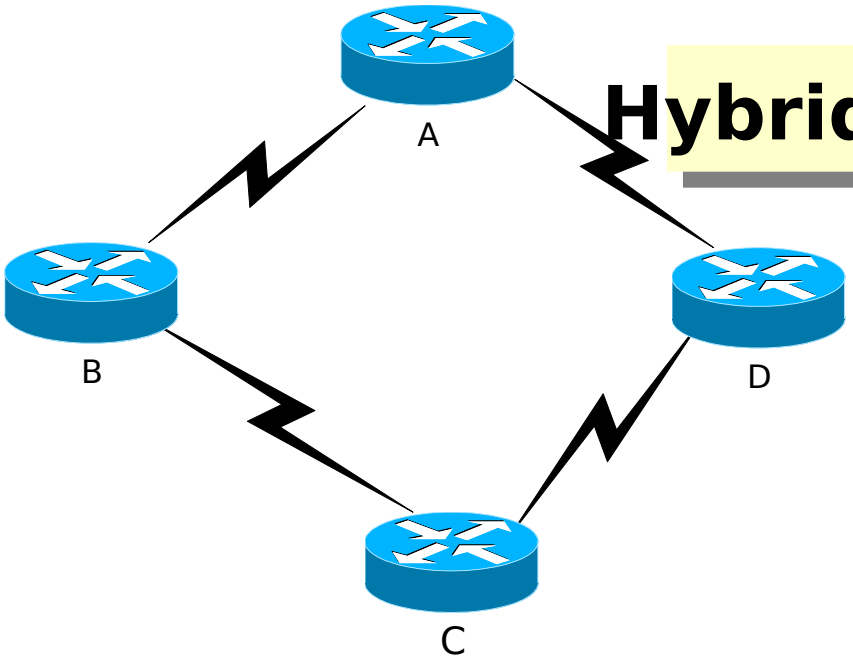
45 Min.

Classes of Routing Protocols

Distance Vector



Hybrid Routing



Link State

Which Protocol?

Issue: Time to Convergence

Convergence occurs when all routers use a consistent perspective of network topology

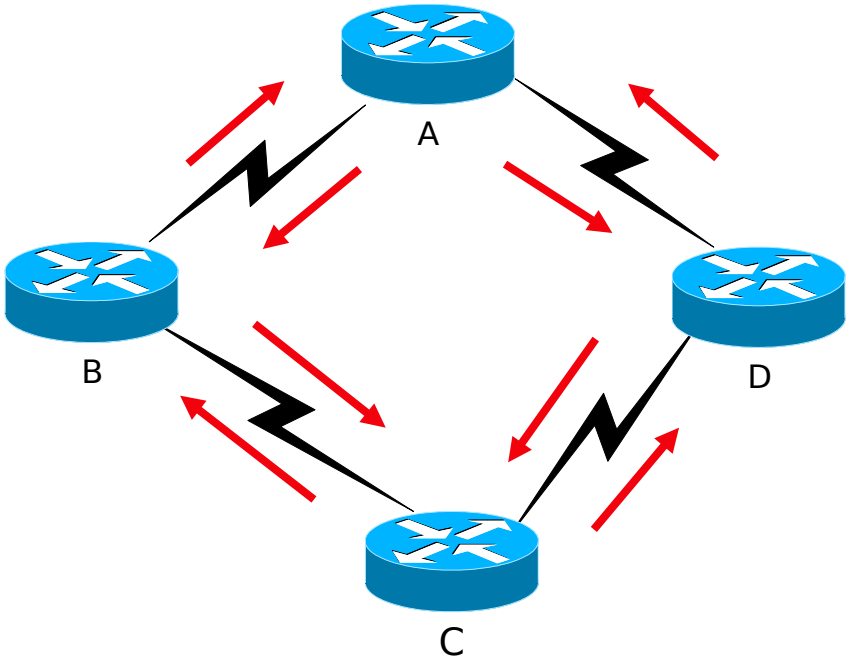
After a topology change, routers must recompute routes, which disrupts routing

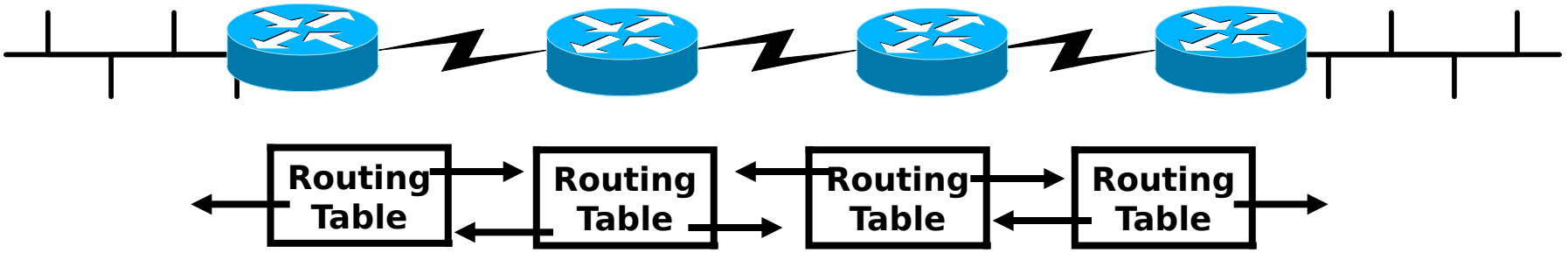
The process and time required for router reconvergence varies in routing protocols

Distance Vector Concept

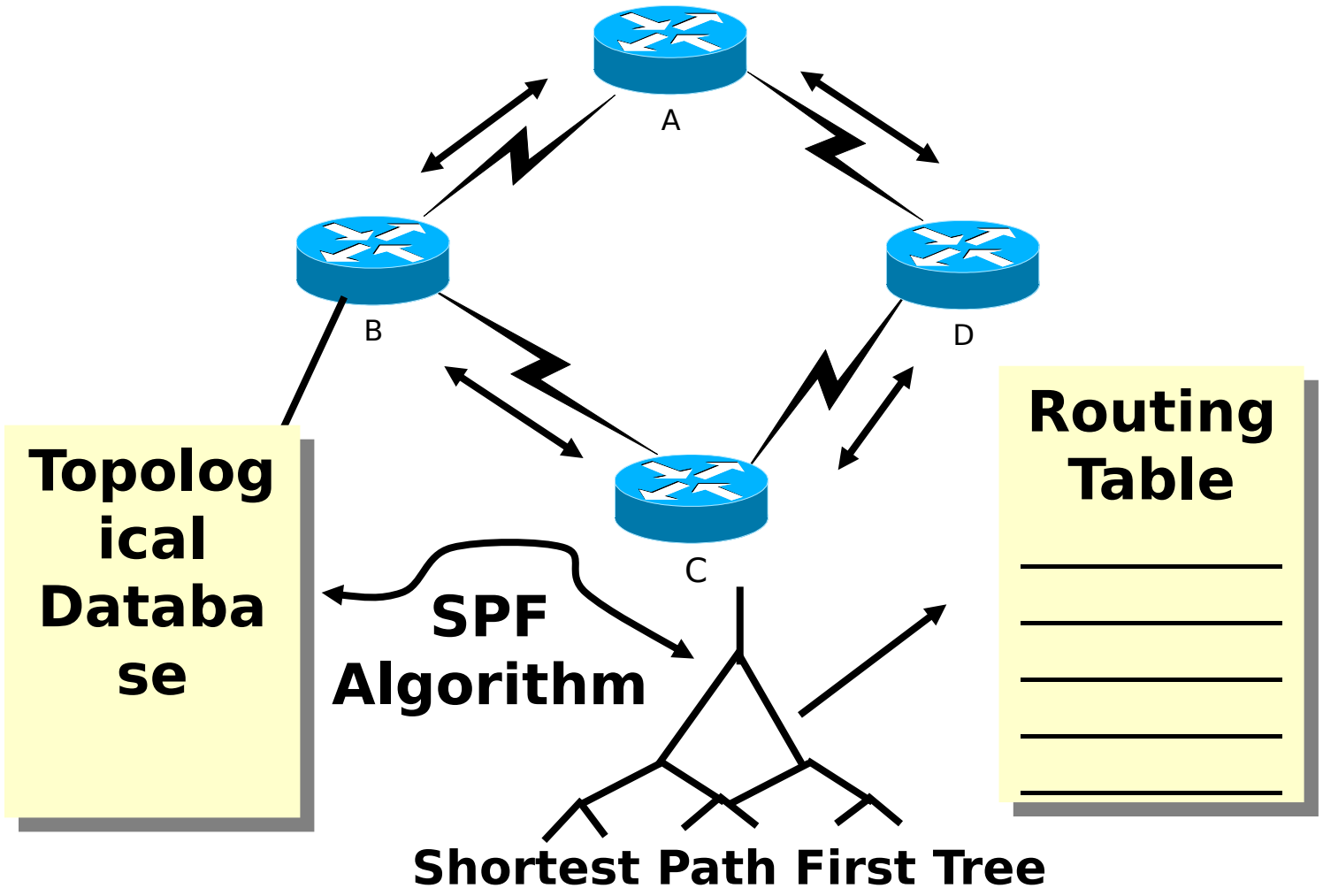
Pass periodic copies of routing table to neighbor routers and accumulate distance vectors

RIP, IGRP, EIGRP





Link-State Concept



Distance Vector vs. Link-State

MSTP

Distance Vector	Link-State
• Views net topology from neighbor's perspective • Adds hop count value • Frequent, periodic updates: slow convergence • Passes copies of routing table to neighbor routers	• Gets common view of entire network topology • Calculates best shortest path to other routers • Event-triggered updates: faster convergence • Passes link-state routing updates to the other routers

What is Best? It Depends

Issues	Concern	Example Questions
Technical	Performance to meet specific needs	Metrics adequate for network size? Any load sharing?
Business	Conformity with enterprise policies and priorities	Proven technology? Multi-vendor support? Standards based?
Operational	Simplicity of	Easy to

th routing protocols, no one type fits all networks

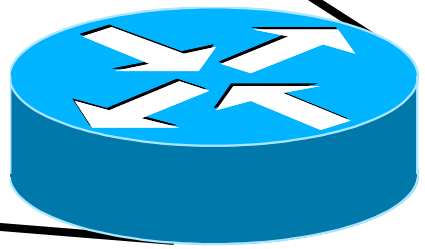
Hybrid Routing

Choose a routing path based on distance vectors

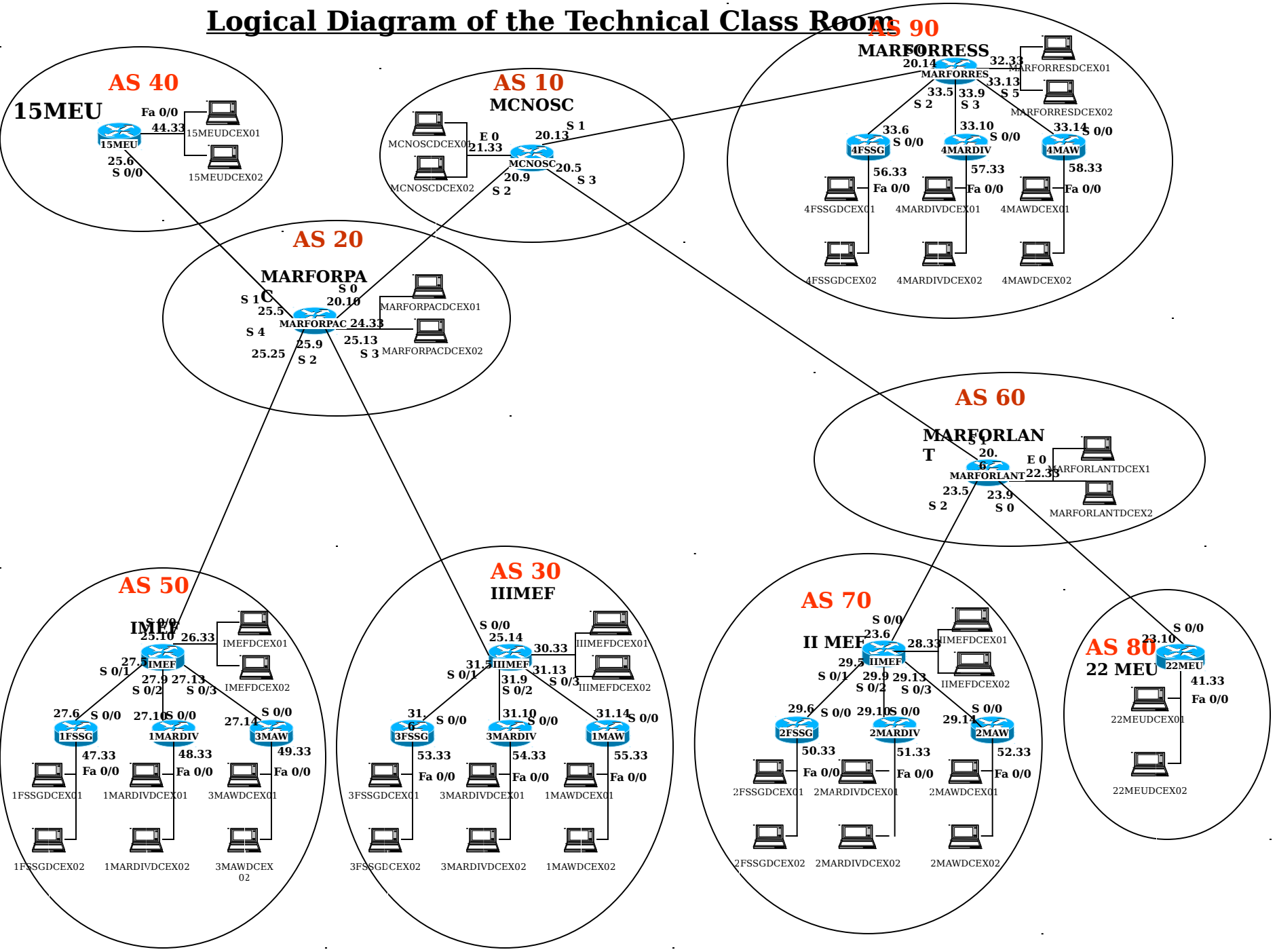
Balanced Hybrid Routing

Converge rapidly using changed-based updates

Share attributes of both distance-vector and link-state routing



Logical Diagram of the Technical Class Room



Routing Protocols

- Determine the "best" route to each destination network
- Distribute routing information amongst systems
- Distribute reach ability information amongst systems
  - Interior routing protocol
    - Interior to an autonomous system
    - Under a common administration
    - Chosen by autonomous system's administrator
  - Exterior routing protocol
    - Between autonomous systems
    - Not under a common administrator

Autonomous System

- An autonomous system is a collection of networks under a common administration sharing a common routing strategy. An autonomous system may comprise of one or many networks, and each network may or may not have an internal structure (subnetting).
- The AS number, which is assigned by the NIC, is a 16-bit decimal number that is uniquely assigned.
- An assigned AS is required in order to run BGP, IGRP, or EIGRP.

Examining Protocols

- "Show Protocol" command (sh ip protocol)
  - Tells which protocols have been turned on globally.
  - Tells what protocols are turned on for each interface, and current status.

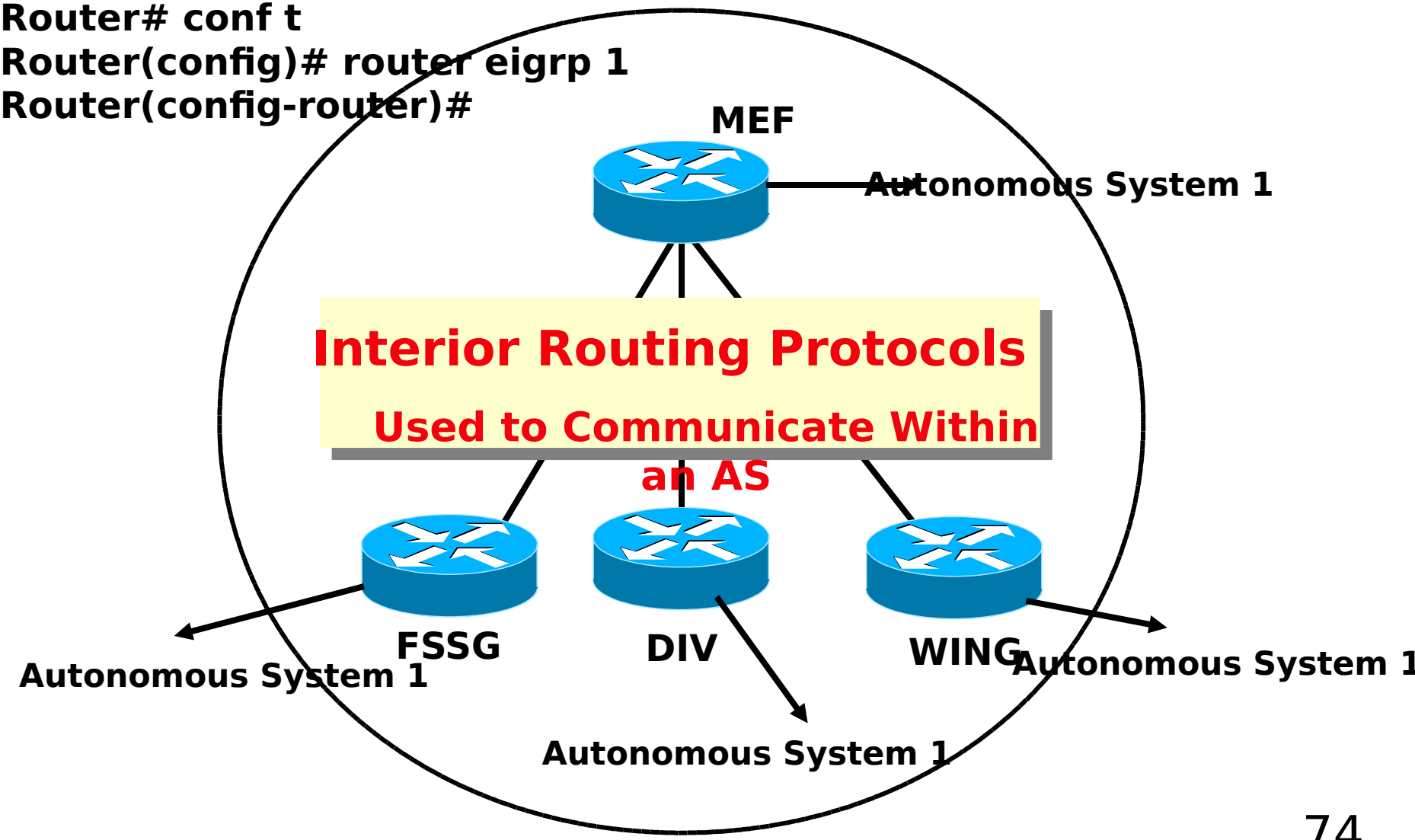
```
sho proto
Global values:
  Internet Protocol routing is enabled
        Serial0 is up, line protocol is up
        Serial1 is administratively down, line
protocol is down
Serial2 is administratively down, line
protocol is down
        Serial3 is administratively down, line
protocol is down
        Ethernet0 is up, line protocol is up
           Internet address is 199.199.199.34
255.255.255.240
        Ethernet1 is up, line protocol is up
           Internet address is 199.199.199.49
```

Listing Routing Protocols

```
MSTP_Unclass#sh ip prot
Routing Protocol is "eigrp 637"
  Outgoing update filter list for all interfaces is
  Incoming update filter list for all interfaces is
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0,
     K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
  Redistributing: eigrp 637
  Automatic network summarization is not in effect
  Routing for Networks:
    138.156.0.0
  Routing Information Sources:
    Gateway         Distance      Last Update
    138.156.169.21       90      00:03:07
    138.156.169.20       90      00:03:07
    138.156.169.4        90      00:03:07
    138.156.169.2        90      00:03:07
    Gateway         Distance      Last Update
    138.156.169.1        90      00:03:08
  Distance: internal 90 external 170
```

Interior Routers

Router# conf t
Router(config)# router eigrp 1
Router(config-router)#



Interior Routing Protocols

- Interior Routing Protocols
  - RIP (Routing Information Protocol)
    - distance vector protocol
    - uses hop counts to determine routing metrics
    - sends out routing broadcasts every 30 seconds
    - small WANs that communicate over fast links
    - from the global configuration

      HOSTNAME(conf)#router rip

      HOSTNAME(conf-router)#network [*ip network*]

Internetworking Cisco Routers

Lab 6.1

Routing Protocols

10 Min.

Interior Routing Protocols

- IGRP (Interior Gateway Routing Protocol)
  - developed by Cisco
  - large diverse networks
  - distance vector
  - from the global configuration mode
    HOSTNAME(conf)#router igrp [*AS*]
    HOSTNAME(conf-router)#network [*ip network*]

Interior Routing Protocols

- EIGRP (Enhanced Interior Gateway Routing Protocol)
  - developed by Cisco
  - distance vector
  - sends out only updates when they happen vice whole tables every 30 seconds
  - supports VLSM
  - from global configuration

  HOSTNAME(conf)#router eigrp [*AS*]

  HOSTNAME(conf-router)#network [*ip network*]

Internetworking Cisco Routers

Lab 6.2, 6.3

Routing Protocols

10 Min.

Interior Routing Protocols

- OSPF (Open shortest path first)
  - RFC 1131 & 1247
  - Supports multiple routes to a destination
    - Supports load balancing
    - Supports variable length subnet mask
    - Supports route summarization
  - Link-state protocol
  - Software is more complex
  - Each node contains map of entire network (overhead)

Configuring Interior Routing

- All IP routing protocols must have a list of networks specified by the network router subcommand before routing activities can begin.
- IGRP and EIGRP require a unique autonomous system number assigned by the NIC (Assigned by MITNOC for USMC).
- Example configuration:
  - router igrp 110 (110 is the unique AS for this network)
  - network 131.108.0.0 (Class B network 131.108 is directly connected and will be broadcast to AS 110)
  - network 192.31.7.0 (Class C network 192.31.7 is also directly connected and will be broadcast)

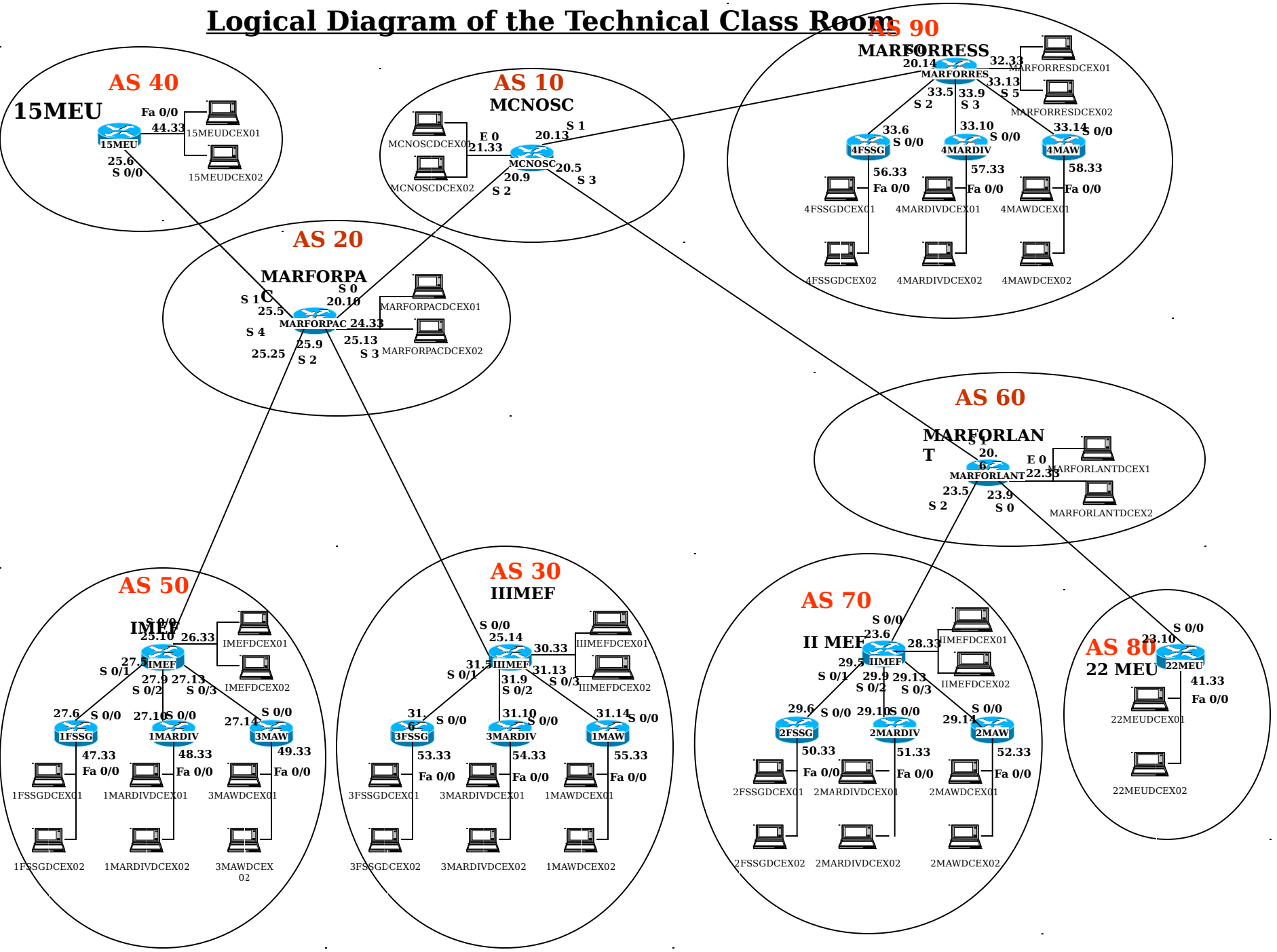
Internetworking Cisco Routers

Lab 6.4

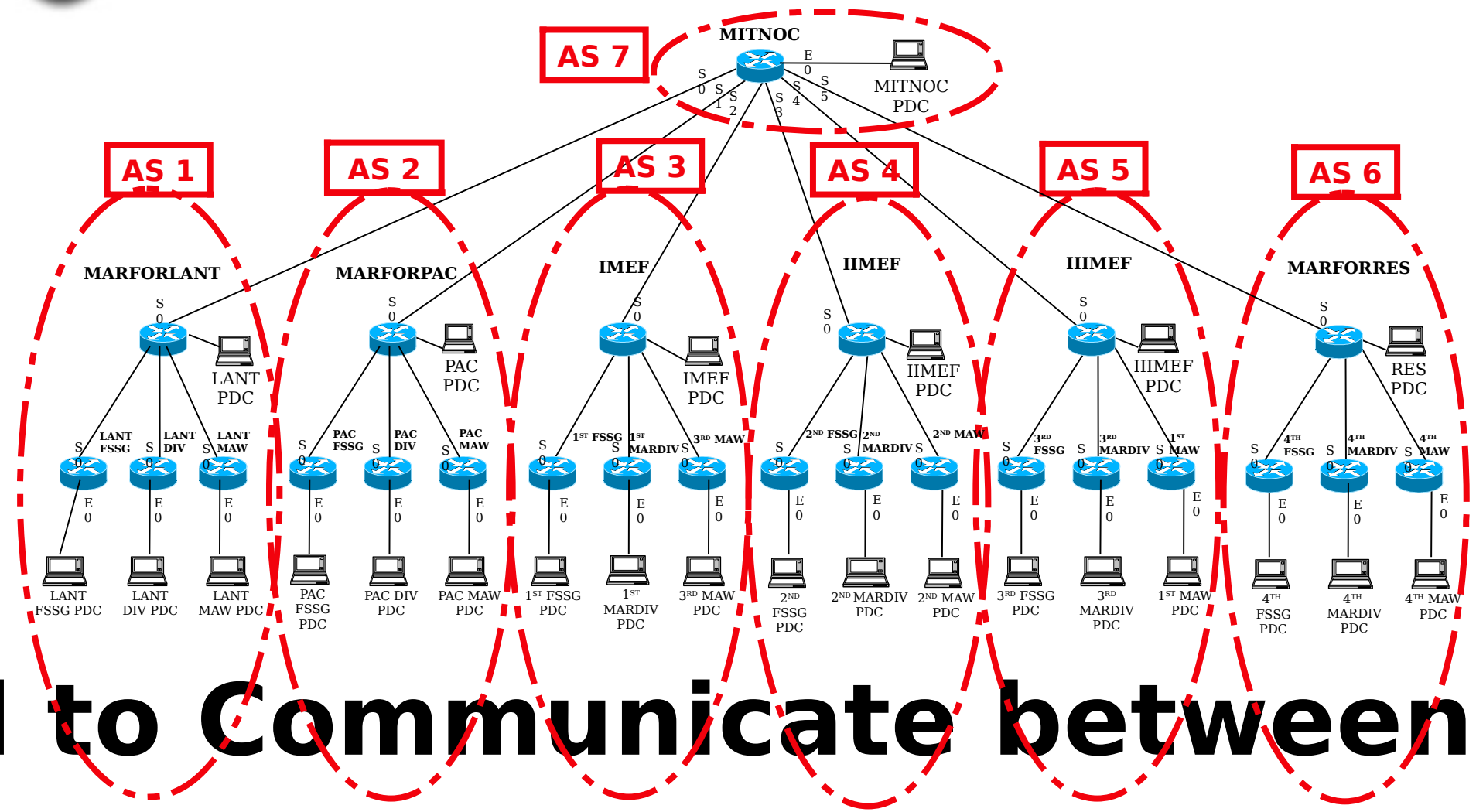
Routing Protocols

10 Min.

Logical Diagram of the Technical Class Room

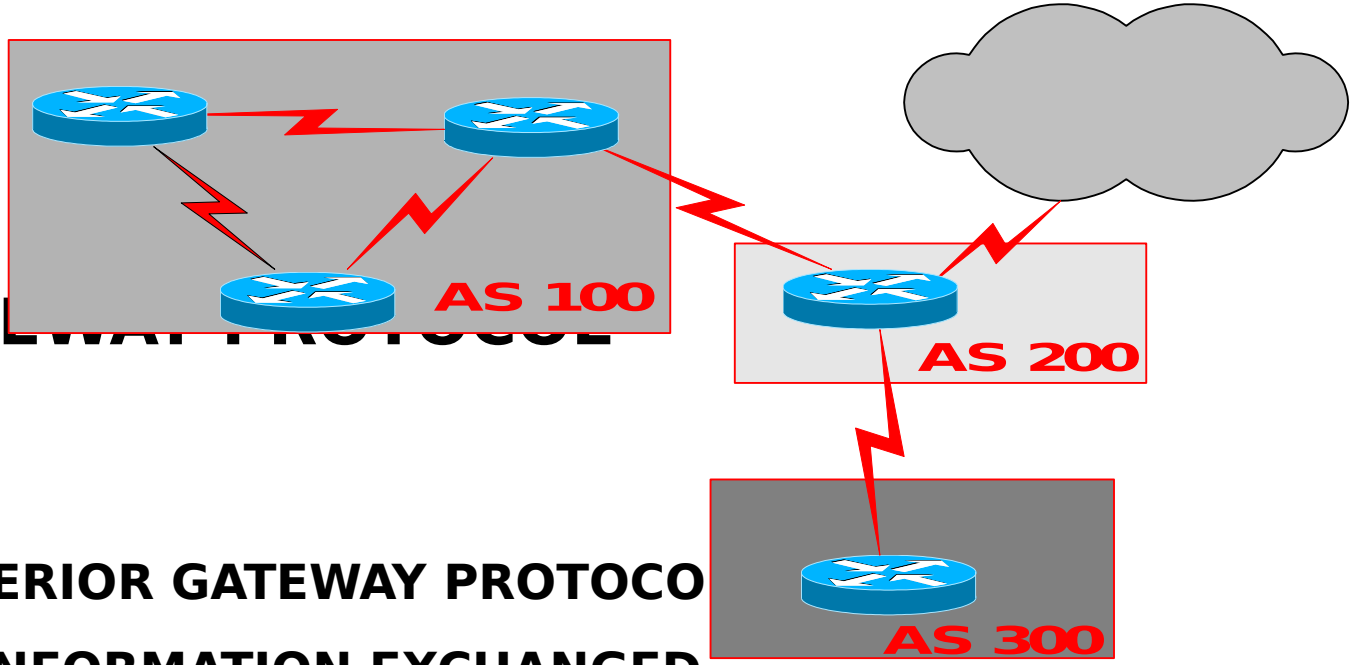


Exterior Routers



l to Communicate between

Exterior Protocols (BGP)



BORDER GATEWAY PROTOCOL (BGP) 4

- **RFC 1267**
- **REPLACING EXTERIOR GATEWAY PROTOCO**
- **REACHABILITY INFORMATION EXCHANGED**
- **MULTIPLE ROUTES SUPPORTED**
- **METRICS USED FOR ROUTING LOOPS AND LOAD BALANCING**
- **ONLY CHANGES ARE SENT AFTER INITIAL EXCHANGE**

Configuring Exterior Routing

- Configuring exterior routing protocols requires three sets of information.
  - A list of neighbor (or peer) routers with which to exchange routing information. This list is created with the neighbor router subcommand
  - A list of networks to advertise as directly reachable, created with the network router subcommand.
  - The AS number of the local router.
- Example BGP Configuration (> ver 4)
  - router bgp 110 (your local AS #)
    network 131.108.0.0 mask 255.255.0.0 (network you wish to advertise)
    neighbor 131.108.100.2 remote-as 109 (IP of router in AS 109)

Internetworking Cisco Routers
Lab 6.5
Routing Protocols

15 Min.

Sources of Routing Information

- Static routes
  - Manually configured by administrator
- Dynamic routing protocols
  - Interior gateway protocols

    RIP, IGRP,OSPF, EIGRP
  - Exterior gateway protocols

    BGP, EGP, EIGRP
- Specifying default routes
  - May be required if router does not know all routes to all networks
  - Can be configured manually in required routers
  - Can be distributed by dynamic protocols

    Displayed in table as “gateway of last resort”

Default Routing

- Manually configuring a static

```
R1# (config) ip route 0.0.0.0 0.0.0.0 192.168.10.1
```

- Source a default route via IGP
  - Define a static route on one router
  - Redistribute static route into IGP

```
R1# (config) #ip route 0.0.0.0 0.0.0.0 192.168.10.1
R1# (config) #router rip
R1# (config-router) #redistribute static
```

- Specifying a default network
  - IGP will decide “best” route to default network

```
R1# (config) #ip default-network network-number
```

Redistributing Data

- Redistributing is the concept of passing unlike protocol information through different routing protocols. An example is IGRP will talk to all other IGRP clients, if you wish to also let those IGRP clients know about the manually added static routes on a router you would enter redistribute static as a router subcommand under the IGRP definition.

ip route 192.1.2.0 192.31.7.65 (static route)

ip route 193.62.5.24 255.255.255.248 192.31.7.65 (static route)

router igrp 110 (shares routing information with AS 110)

network 192.31.7.0 (locally connected network)

redistribute static (passes the two static routes as well)

redistribute rip (pass all RIP learned

Default Metric

The following example takes redistributed RIP metrics and translates them into EIGRP metrics with values as follows:

bandwidth = 1000
delay = 100
reliability = 250
loading = 100
mtu =1500

router eigrp 109
network 131.108.0.0
redistribute rip
default-metric 1000 100 250 100 1500

Routing Protocol Weights

The weight of a protocol helps the router to decide which is the

Directly Connected	0
Static	1
BGP (external)	20
EIGRP (internal)	90
IGRP	100
OSPF	110
RIP	120
EGP	140
EIGRP (external)	170
BGP (internal)	200
Unknown	255

DECISION PROCESS

NETWORK	VIA	HOW	DISTANCE	METRIC
199.112.104.0	S1	EIGRP 5343	90	200000
199.112.104.0	S2	EIGRP 5343	90	250000
199.112.104.0	S3	IGRP 5343	100	200000
199.112.100.0	E0	CONNECT	0	
199.112.101.0	S1	EIGRP 5343	90	250000
199.112.101.0	S2	EIGRP 5343	90	200000
199.112.101.0	S3	IGRP 5343	100	200000
199.112.102.0	E0	STATIC	1	

ROUTING TABLE

NETWORK	VIA	HOW	DISTANCE	METRIC
199.112.104.0	S1	EIGRP 5343	90	200000
199.112.100.0	E0	CONNECT	0	
199.112.101.0	S2	EIGRP 5343	90	200000
199.112.102.0	E0	STATIC	1	

Routing Decisions

- The Decision table ensures a dynamic route change in the case one or more paths to a network should fail.
- The more routing protocols being run, the larger the table. This uses valuable bandwidth and memory
- The router will keep which protocol it learned the route from for redistribution purposes.
- The routing table keeps only one entry for each network.

Security Issues

- Password Security
- Keeping Out Unwanted Guests
- Allowing Certain Information

Password Security

- Password security is crucial for network integrity. It is recommended to mix the cases of the letters, and using "special characters" also helps in warding off hackers. Example: 2b,OR#2b.
- Never keep copies of configurations laying around that still display the passwords. Always edit the file after loading it onto a local drive.
- Outside administrators can still view most information without needing to know the Enable password. Always offer just a terminal login password unless they need to reconfigure as well.

Recovering Lost Passwords (2600/3600 Series)

- Power cycle the router
- Press the break key within 60 seconds (from console port only)
- other break definitions: Windows - ^$B, Procomm- Alt B, ASC - ^C
- Record original software configuration register value
- >Confreg 0x2142 [CR]
- >i [CR]
- Answer no to all of the SETUP questions
- Route>enable [CR]
- Router#Copy Start Run [CR]
- Hostname(Config)#enable secret *password*
- Record passwords for console, vty ports, and enable
- Hostname(Config)#config-register 0x2102
- Must execute the command “no shut” on all interfaces
- Hostname#Copy Run Start
- #reload [CR] or power cycle router (say NO if asked to save)

Recovering Lost Passwords (2000/4000 Series)

- Power cycle the router
- Press the break key within 60 seconds (from console port only)
- other break definitions: Windows - ^$B, Procomm- Alt B, ASC - ^C
- >e/s 2000002 [CR] q [CR]
- Record original software configuration register value
- >o/r 0x2142 [CR]
- >i [CR]
- Answer no to all of the SETUP questions
- >enable [CR]
- #show configuration [CR]
- Record passwords for console, vty ports, and enable
- #reload [CR] or power cycle router (say NO if asked to save)
- Press the break key within 60 seconds
- >o/r 0x(original value, 2102 is standard) [CR]
- >i [CR]

Access Lists

- Access Lists determine what type of traffic is or is not allowed to travel through certain ports.
- Several Access Groups can be made to allow for different settings for particular ports or groups of ports.
- Some basic rules of access lists:
  - access commands are dependent on order of entry
  - if a packet meets any condition it is approved, else it is denied and is not sent out the port.
  - restrictions can be set to either incoming or outgoing traffic. Be sure to set the lists in the right direction.
  - It is usually best to use reverse logic for restrictions. That is to say, restrict all traffic, then set what is allowed.

Access List


```
interface Ethernet 0
ip address 143.211.80.1 255.255.255.0 secondary
ip address 143.211.14.1 255.255.255.0
ip access-group 105 out

access-list 102 permit ip 143.211.0.0  0.0.255.255  0.0.0.0  255.255.255.255
access-list 102 permit tcp 0.0.0.0  255.255.255.255  143.211.0.0  0.0.255.255
    established
access-list 102 permit icmp 0.0.0.0  255.255.255.255  143.211.0.0  0.0.255.255
access-list 102 permit tcp 0.0.0.0  255.255.255.255  143.211.0.0  0.0.255.255 gt 1000
access-list 102 permit udp 0.0.0.0  255.255.255.255  143.211.0.0  0.0.255.255 gt 1000
access-list 102 permit tcp 0.0.0.0  255.255.255.255  143.211.90.50  0.0.0.0 eq 25
access-list 102 permit tcp 0.0.0.0  255.255.255.255  143.211.90.50  0.0.0.0 eq 520
access-list 102 permit tcp 0.0.0.0  255.255.255.255 143.211.90.51  0.0.0.0 eq 119
access-list 105 permit tcp 0.0.0.0  255.255.255.255  143.211.0.0  0.0.255.255
    established
access-list 105 permit tcp 0.0.0.0  255.255.255.255  143.211.0.0  0.0.255.255 gt 1024
access-list 105 permit icmp 0.0.0.0  255.255.255.255  143.211.0.0  0.0.255.255
access-list 105 permit ip 143.211.0.0  0.0.255.255  0.0.0.0  255.255.255.255
access-list 105 permit udp 0.0.0.0  255.255.255.255  143.211.0.0  0.0.255.255 gt 1000
```

Access List In Detail

- List out your goals, and check off each item as you fulfill that goal.
- Simple access list (1-99)

 # source/dest valid

access-list 1 permit ip 192.156.69.0 0.0.0.255

- Extended access list (100-199)

 # source valid dest valid

access-list 101 permit ip 192.156.69.0 0.0.0.255 0.0.0.0 255.255.255.255

access-list 101 permit ip 0.0.0.0 255.255.255.255 192.156.69.0 0.0.0.255 eq 25

- Assigning access groups to interfaces

int e 1

ip access-group 101 [in/out]

Access List In Detail

- How the validation mask works
  - 0=Exact Match
  - 1=Don't care

Matching a whole network

192.156.69.0= 1000000.10011100.01000101.00000000

0.0.0.255 = 00000000.00000000.00000000.11111111

Matching a subnet: Example for 4 bit mask

192.156.69.32= 1000000.10011100.01000101.00100000

0.0.0.15 = 00000000.00000000.00000000.00001111

128	64	32	16	8	4	2	1	
0	0	1	0	0	0	0	0	32 Network
0	0	1	0	0	0	0	1	33 1st host
0	0	1	0	0	0	1	0	34 2nd host
0	0	1	0	1	1	1	1	47 Broadcast
0	0	1	1	0	0	0	0	48 No longer matches mask

Internetworking Cisco Routers

Lab 7

Access Lists

45 Min.

Advance Topics

MSTP

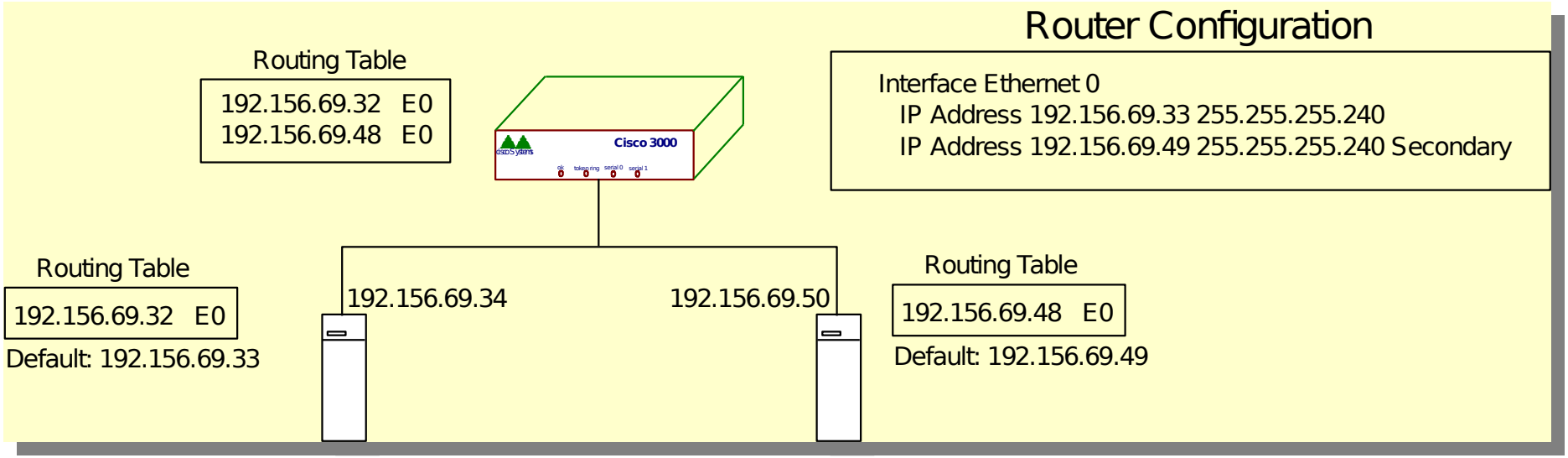
- Secondary Addresses
- Collapsing Backbones
- CIDR/Supernetting
- VLSM
- Queuing

Multiple Networks On The Same Line

- Should only be used when migrating
- Benefits
  - Allows for easy migrations
  - Works well for systems that use the broadcast address to advertise to clients, such as GCCS.
- Costs
  - Very inefficient at routing

Multiple Networks On The Same Line

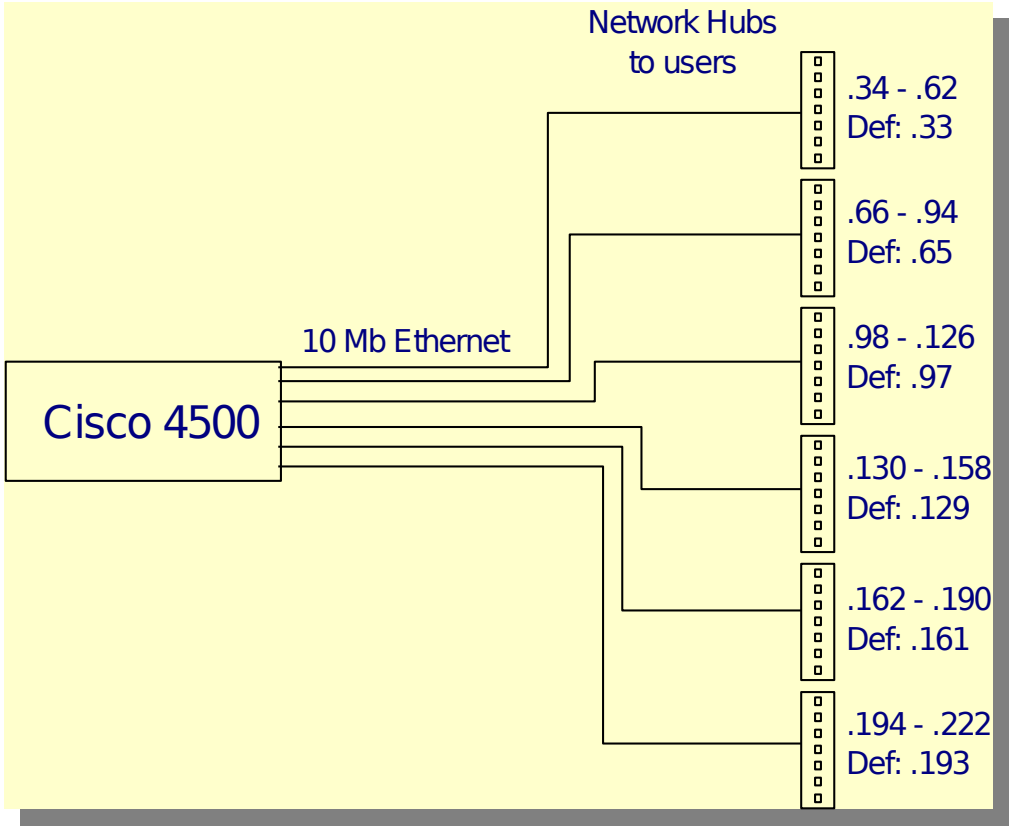
- Trace the network traffic between devices:
- Both workstations work fine when sending traffic to the router (default).
- When sending to each other, each workstation sends the traffic to the router first because the other workstation is not a known network.



Collapsing Backbones

elow represents a six port ethernet router with a 3 bit subne

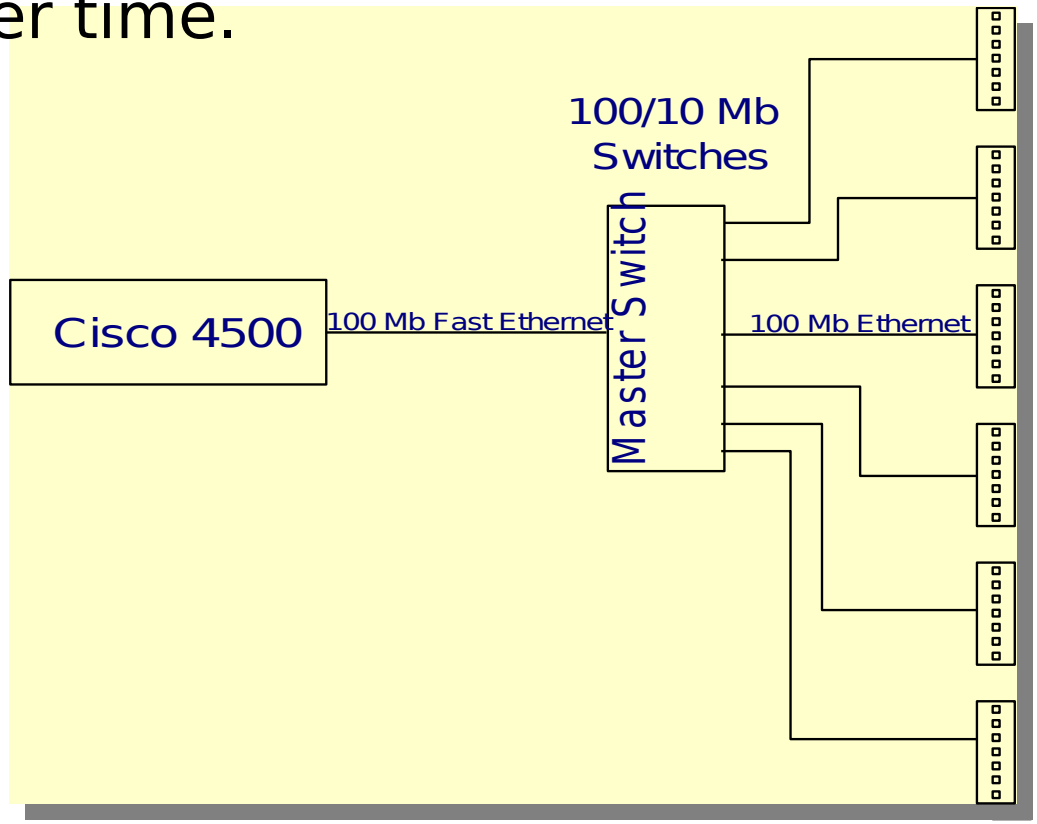
Interface Ethernet 0
IP Address 192.156.69.33 255.255.255.224
Interface Ethernet 1
IP Address 192.156.69.65 255.255.255.224
Interface Ethernet 2
IP Address 192.156.69.97 255.255.255.224
Interface Ethernet 3
IP Address 192.156.69.129
255.255.255.224
Interface Ethernet 4
IP Address 192.156.69.161
255.255.255.224
Interface Ethernet 5
IP Address 192.156.69.193
255.255.255.224



Collapsing Backbones

Changing the subnet mask to 255.255.255.0 and assigning secondary addresses or subinterfaces of the original defaults allows the administrator to migrate the users over time.

```
Interface Fastethernet 0
   IP Address 192.156.69.1 255.255.255.0
   IP Address 192.156.69.33 255.255.255.0 Secondary
   IP Address 192.156.69.49 255.255.255.0 Secondary
   IP Address 192.156.69.65 255.255.255.0 Secondary
   IP Address 192.156.69.97 255.255.255.0 Secondary
   IP Address 192.156.69.129 255.255.255.0 Secondary
   IP Address 192.156.69.161 255.255.255.0 Secondary
   IP Address 192.156.69.193 255.255.255.0 Secondary
```



Supernetting/CIDR

MSTP

- Supernetting and Classless Inter Domain Routing (CIDR) reduce routing tables by grouping or blocking networks.
- Determine common network bits
- Write networks out in binary
- Turn all common network bits to 1 to determine supernet
- Count number of common bits for CIDR mask

204.223.0.0 = 11001100.11011111.00000000.00000000
204.223.1.0 = 11001100.11011111.00000001.00000000
204.223.2.0 = 11001100.11011111.00000010.00000000
204.223.3.0 = 11001100.11011111.00000011.00000000

Common Network Bits

11111111.11111111.11111100.00000000 255.255.252.0 or /22

Supernet Mask CIDR

Supernetting/CIDR

- Determining The Maximum Block Size
- Write last octet in binary value
- Go to last active bit to determine magic number

	128	64	32	16	8	4	2	1	Max Block
160	1	0	1	0	0	0	0	0	32
161	1	0	1	0	0	0	0	1	1
162	1	0	1	0	0	0	1	0	2

- Blocking networks
- Block from network 204.223.150.0 - 204.223.180.0

	128	64	32	16	8	4	2	1	Block/Max	Possible	CIDR	Supernet
150	1	0	0	1	0	1	1	0	2/2	.150-151	/23	255.255.254.0
152	1	0	0	1	1	0	0	0	8/8	.152-159	/21	255.255.248.0
160	1	0	1	0	0	0	0	0	16/32	.160-175	/20	255.255.240.0
176	1	0	1	1	0	0	0	0	4/16	.176-179	/22	255.255.252.0
180	1	0	1	1	0	1	0	0	1/4	.180-180	/24	255.255.255.0

VLSM

- Variable Length Subnet Mask (VLSM) is the practice of using multiple network masks for the same network
- You must start with the largest blocks and divide those blocks into smaller subnets
- Allows backbone routing tables to be smaller, while giving the individual unit the flexibility of their own subnet scheme
- Currently supported by EIGRP and OSPF

Upgrading a Router's Software

- Prepare router with newest software revision
  - Use "show ver" to find the name of the image file
  - Allow router to serve as a tftp site
    - conf t
    - tftp-server system [image file]
- Prepare router with older software revision
- For permanent upgrade to router
  - copy tftp flash (will run through several questions)
  - enter IP address of tftp router, and image name
  - will erase old flash and copy new image file over (bad time for the network to go down!)
  - reload
  - wr mem (to save config under current revision)

Recovering From a Bad Upgrade

- Boot to ROM Monitor
- Use "Break key" on startup
- Terminal:^C ProComm:Alt-B Windows:^$B
- Configure to boot from ROM bootstrap
- o/r 0x101
- i (initiate)
- Replace original software revision
- copy tftp flash
- enter IP address of router with original version of software
- reload
- Reset Configuration Register from ROM Monitor
- o/r 0x2102
- i

Software Upgrade Safety Tips

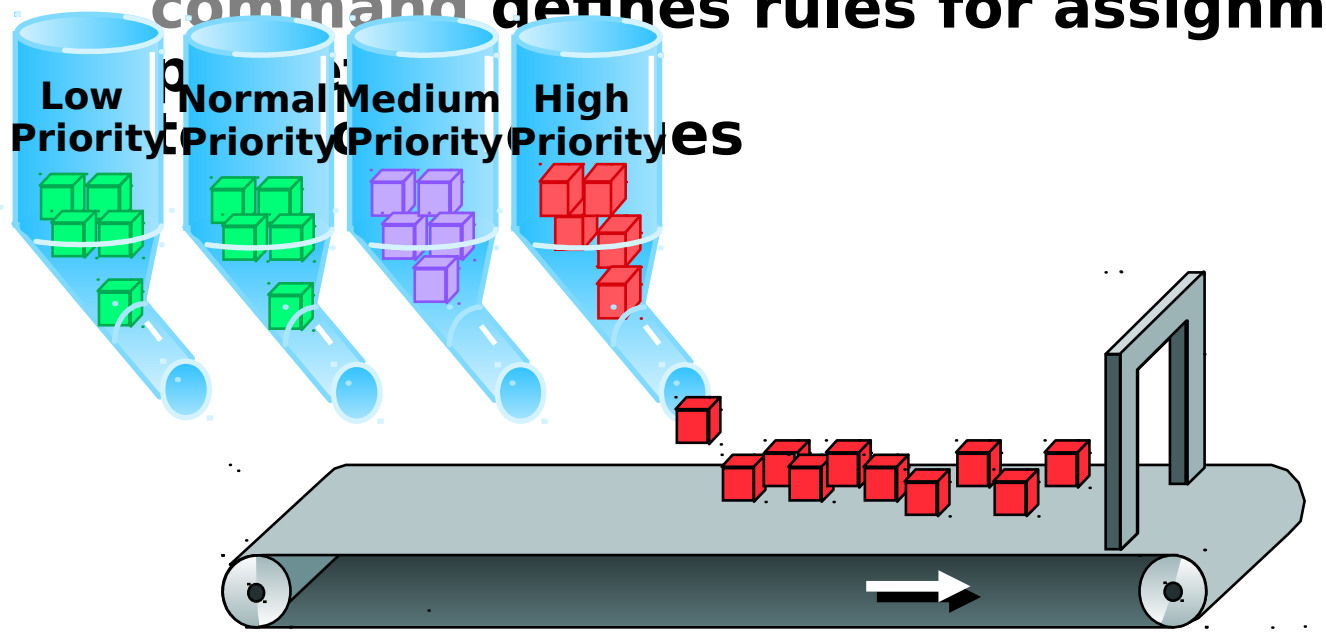
- It is best to do the upgrade with three routers.
- one with the newest software, two with the older software, so should it fail, there is a backup router with the original software
- When only two routers available (1 new, 1 old)
- Allow older router to serve as tftp server
- conf t
- tftp-server system [image file name]
- Copy original software image file onto new router
- copy tftp flash
- enter IP address of router with original version of software
- *** DO NOT ERASE OLD FLASH ***
- Allow new router to serve as tftp server for both images
- tftp-server system [older image file]
- tftp-server system [older image file]

Queuing

- The Cisco IOS implements four (now five) different queuing algorithms today:
  - First in, First Out (FIFO) Queuing
  - Priority Queuing
  - Custom Queuing
  - Weighted Fair Queuing
  - Class Based Weighted Fair Queuing
  - Interleave with Fragmentation
- Queuing occurs when network congestion occurs (i.e., the queue depth => 1), else all packets are sent as they arrive at the interface

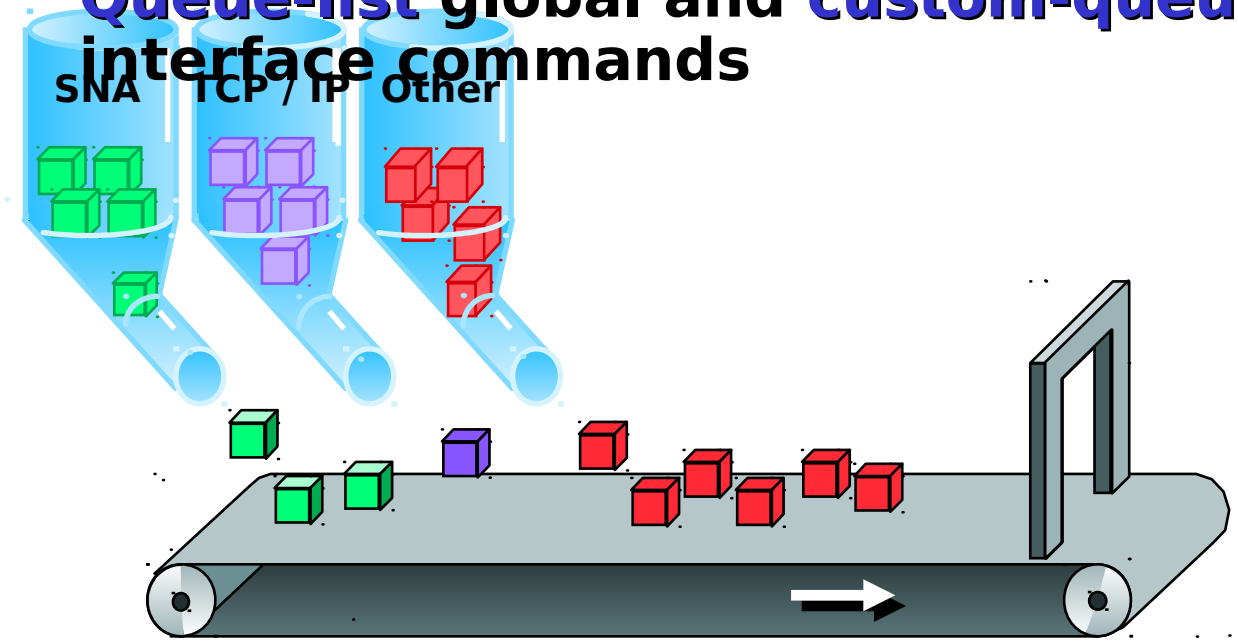
Priority Queuing

- **Four queues: high, medium, normal and low**
- **Priority-list global and priority-group interface command defines rules for assignment of packets to queues**



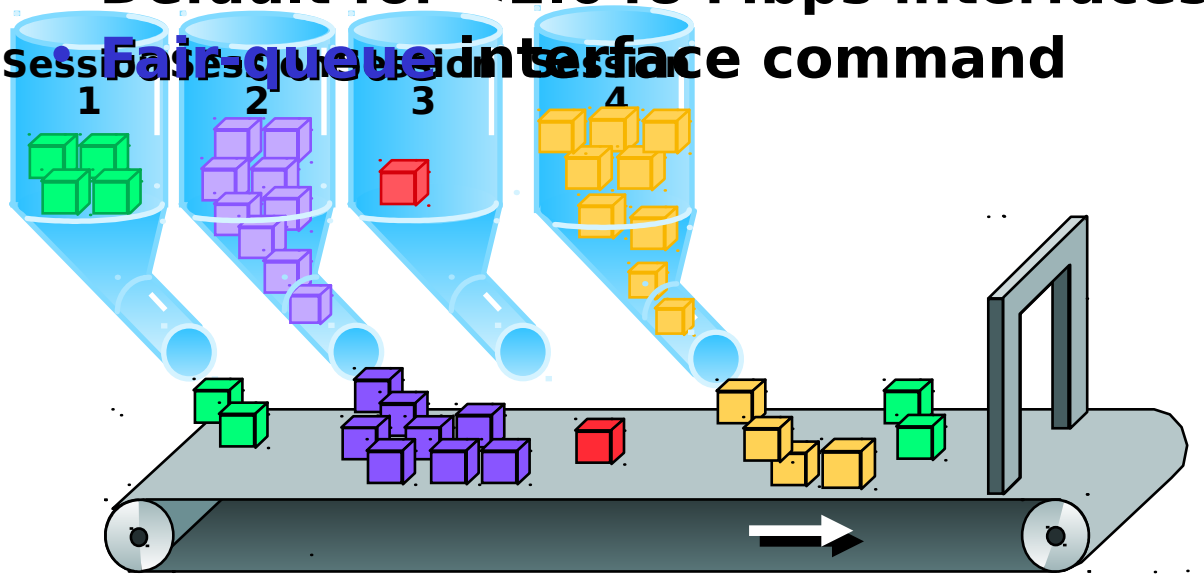
Custom Queuing

- **Control % of interface bandwidth for specified traffic**
- **17 output queues for each interface [16 configurable]**
- **Queue-list global and custom-queue-list interface commands**



Weighted Fair Queuing

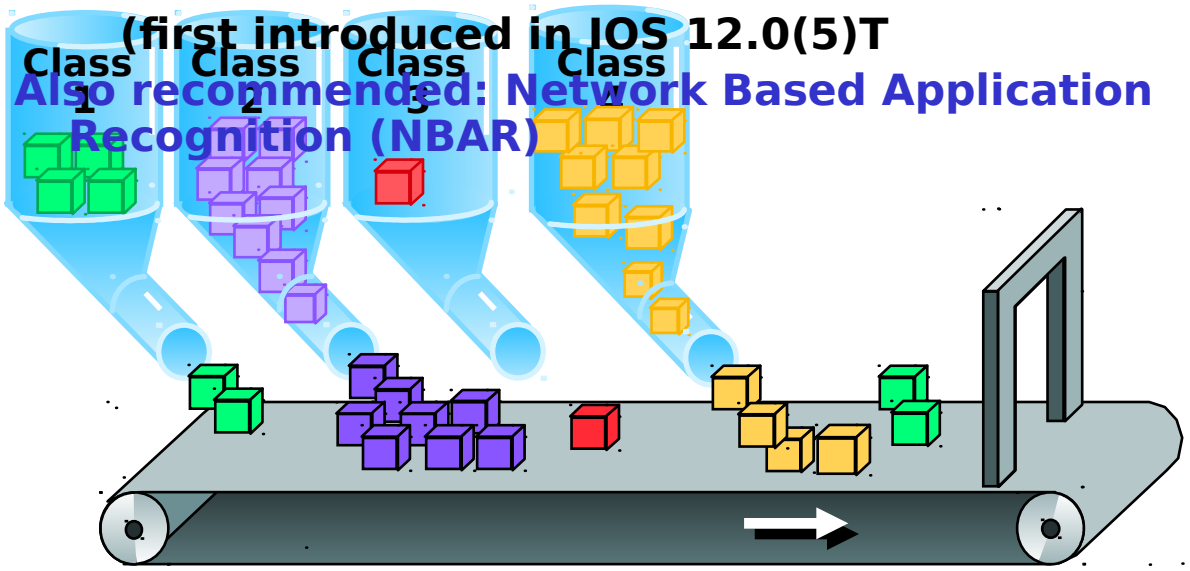
- **Automatic traffic priority management**
- **Low-bandwidth sessions have priority over high-bandwidth sessions**
- **High-bandwidth sessions assigned weights**
- **Default for <2.048 Mbps interfaces**
- **Fair-queue interface command**



Class Based Weighted Fair Queuing

- **Class Based traffic priority management**
- **Administrators can assign priority and Bandwidth to Classes of Traffic**
- **Requires the MCL**
- **Requires: The Modular QOS Command Line Interface**
  (first introduced in IOS 12.0(5)T

Also recommended: Network Based Application Recognition (NBAR)



Internetworking Cisco Routers

Lab 8

Putting it all together

45 Min.